CONTENTS DATA EVALUATING DEVICE

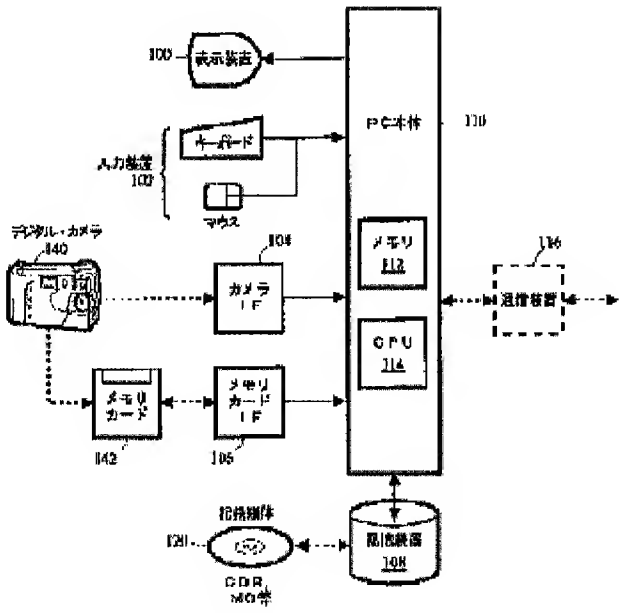
Publication number: JP2001036856
Publication date: 2001-02-09
Inventor: TOYOKAWA KAZUHARU; MORIMOTO NORISHIGE; TONEGAWA SATOKO
Applicant: IBM
Classification:
- international: ***H04N5/91; G06F7/04; G06K9/00; H04L9/32; H04N1/387; H04N7/167;*** **H04N5/91; G06F7/02; G06K9/00; H04L9/32; H04N1/387; H04N7/167;** (IPC1-7): H04N5/91; H04N1/387
- European:
Application number: JP19990176094 19990622
Priority number(s): JP19990176094 19990622

Also published as:
US6829367 (B1)
CA2307534 (A1)

Report a data error here

Abstract of **JP2001036856**

PROBLEM TO BE SOLVED: To accurately judge which part of contents data are altered since the time of preparing them by providing a means for sampling data for specifying contents and a means for judging the presence/absence of the alteration of the contents data based on this sampling result. SOLUTION: A picture alteration judging device compress-encodes a picture photographed by a digital camera 140 by a JPEG system, e.g. to accept via a camera IF 104. Otherwise, the device accepts compressed picture data recorded in a memory card 142 by the camera 140 through a memory card IF106. At the time of accepting the compressed picture data, an electronic watermark (embedded data) is embedded to the compressed picture data. Then, through the use of using the character of JPEG data obtained by embedding the embedded data, a sampling part judges and displays whether the JPEG data are altered or not and when it is altered, the part decides and displays which part of the picture data are altered.



Family list
4 family members for: **JP2001036856**
Derived from 3 applications

Back to JP2001036856

1 **CONTENT DATA JUDGING APPARATUS**
Inventor: TONEGAWA SATOKO (JP); MORIMOTO NORISHIGE (JP); (+1)
Applicant: IBM (US)
EC:
IPC: ***H04N5/91; G06F7/04; G06K9/00*** (+11)
Publication info: CA2307534 A1 - 2000-12-22

2 **CONTENTS DATA EVALUATING DEVICE**
Inventor: TOYOKAWA KAZUHARU; MORIMOTO NORISHIGE; (+1)
Applicant: IBM
EC:
IPC: ***H04N5/91; G06F7/04; G06K9/00*** (+11)
Publication info: JP3342677B2 B2 - 2002-11-11
JP2001036856 A - 2001-02-09

3 **Content data judging apparatus**
Inventor: TOYOKAWA KAZUHARA (JP); MORIMOTO NORISHIGE (JP); (+1)
Applicant: IBM (US)
EC:
IPC: ***H04N5/91; G06F7/04; G06K9/00*** (+11)
Publication info: US6829367 B1 - 2004-12-07

Data supplied from the ***esp@cenet*** database - Worldwide

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（A）　(11)特許出願公開番号
特開2001－36856
（P2001－36856A）
(43)公開日　平成13年２月９日(2001.2.9)

(51)Int.Cl.⁷	識別記号	FI		テーマコード（参考）
H04N 5/91		H04N 5/91	P	5C053
1/387		1/387		5C076

審査請求　有　　請求項の数15　OL　（全 36 頁）

(21)出願番号　特願平11－176094

(22)出願日　平成11年６月22日(1999.6.22)

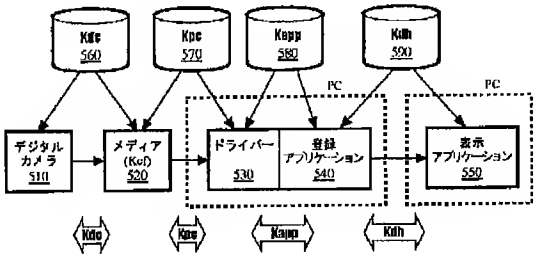
(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
INTERNATIONAL BUSINESS MASCHINES CORPORATION
アメリカ合衆国10504、ニューヨーク州
アーモンク　（番地なし）

(74)代理人　100086243
弁理士　坂口　博　（外１名）

最終頁に続く

(54)【発明の名称】　コンテンツデータ鑑定装置

(57)【要約】　（修正有）
【課題】　コンテンツデータ作成時点からどこが改変されたかを正確に判定する鑑定方法を提供する。
【解決手段】（１）コンテンツデータを記録したメディアと認証を行う手段と、（２）メディアに記録されたコンテンツデータを読み取る手段と、（３）コンテンツデータに、該コンテンツを特定するデータを埋め込む手段と、（４）コンテンツを特定するデータの埋め込まれたコンテンツデータから、該コンテンツを特定するデータを抽出する手段と、（５）コンテンツを特定するデータの抽出結果に基づき、コンテンツデータ改変の有無の判断を行う手段と、コンテンツデータに改変がなされたと判断した場合に、改変個所の特定を行う手段を有する。



【特許請求の範囲】

【請求項１】デジタルデバイスで作成されたコンテンツデータに改変がなされたかどうかを鑑定する、コンテンツデータ鑑定装置であって、（１）コンテンツデータを記録したメディアと認証を行う手段と、（２）前記メディアに記録されたコンテンツデータを読み取る手段と、（３）前記コンテンツデータに、該コンテンツを特定するデータを埋め込む手段と、（４）前記コンテンツを特定するデータの埋め込まれたコンテンツデータから、該コンテンツを特定するデータを抽出する手段と、（５）前記コンテンツを特定するデータの抽出結果に基づき、コンテンツデータ改変の有無の判断を行う手段とを有する、コンテンツデータ鑑定装置。

【請求項２】前記コンテンツデータ改変の有無の判断を行う手段（５）が、コンテンツデータに改変がなされたと判断した場合に、改変個所の特定を行う手段を有する、請求項１記載の装置。

【請求項３】前記コンテンツデータを読み取る手段（２）において、前記メディアに記録されたコンテンツデータが、デジタルデバイスと前記メディアとの認証結果を含み、該認証結果を読み取る手段を有する、請求項１記載の装置。

【請求項４】前記コンテンツを特定するデータ埋め込む手段（３）が、コンテンツデータに、コンテンツデータの認証履歴情報、作成日、作成者、作成機器、登録日などを含むＩＤ情報を埋め込む手段を有する、請求項１記載の装置。

【請求項５】デジタルデバイスで作成されたコンテンツデータに、改変検出用データを埋め込む装置であって、（１）コンテンツデータを記録したメディアと認証を行う手段と、（２）前記メディアに保存されたコンテンツデータを読み取る手段と、（３）前記コンテンツデータに、改変個所の特定を行う改変検出用データを埋め込み、記憶する手段と、を有する、改変検出用データ埋め込み装置。

【請求項６】コンテンツデータ改変鑑定装置であって、（１）改変検出用データの埋め込まれたコンテンツデータから、改変検出用データを抽出する手段と、（２）前記改変検出用データの抽出結果に基づき、コンテンツデータ改変の有無の判断を行い、改変がなされたと判断した場合に改変個所の特定を行う手段と、を有する、コンテンツデータ改変鑑定装置。

【請求項７】前記デジタルデバイスが、カメラ、録音装置、スキャナ、もしくはビデオカメラである、請求項１～請求項５の何れかに記載の装置。

【請求項８】デジタルカメラと、デジタルカメラで作成された画像を記録する記録メディアと、記録メディアにアクセスし画像データを読み取り電子透かしを埋め込む電子透かし埋め込み装置と、画像データに埋め込まれた電子透かしを抽出する電子透かし抽出装置、からなる画像データ鑑定装置であって、（１）デジタルカメラで画像データを作成する手段と、（２）デジタルカメラと画像記録メディア間で認証を行う手段と、（３）前記認証が成功した場合、前記画像データを前記画像記録メディアに記録する手段と、（４）前記記録メディアと電子透かし埋め込み装置間で認証を行う手段と、（５）前記認証が成功した場合、前記電子透かし埋め込み装置が、前記記録メディアから前記画像データを読み取る手段と、（６）前記電子透かし埋め込み装置が、前記画像データに、改変判定のためのデータを、複数の前記認証の結果および画像データに関連するＩＤ情報と共に、電子透かしとして埋め込む手段と、（７）前記電子透かし埋め込み装置が、前記電子透かしの埋め込まれた、前記画像データを記憶装置に記録する手段と、（８）電子透かし検出装置が、前記記憶装置に記録された画像データを読み取り、該画像データに埋め込まれた電子透かしを抽出する手段と、（９）前記電子透かし検出装置が、抽出された前記電子透かしの結果から、前記画像データに改変がなされたかどうかを判断し、改変がなされた判断した場合、改変の個所を特定する手段と、を有する、画像データ鑑定装置。

【請求項９】デジタルカメラで作成された画像を鑑定する方法であって、（１）デジタルカメラで画像データを作成する段階と、（２）デジタルカメラと画像記録メディア間で認証を行う段階と、（３）前記認証が成功した場合、前記画像データを前記画像記録メディアに記録する段階と、（４）前記記録メディアとデバイスドライバ間で認証を行う段階と、（５）前記認証が成功した場合、前記デバイスドライバと、電子透かしを埋め込む電子透かし埋め込みプログラム間で認証を行う段階と、（６）前記電子透かし埋め込みプログラムが、前記記録メディアから前記画像データを読み取る段階と、（７）前記電子透かし埋め込みプログラムが、前記画像データに、改変判定のためのデータを、複数の前記認証の結果および画像データに関連するＩＤ情報と共に、電子透かしとして埋め込む段階と、（８）前記電子透かし埋め込みプログラムが、前記電子透かしの埋め込まれた、前記画像データを記憶装置に記録する段階と、（９）電子透かし検出プログラムが、前記記憶装置に記録された画像データを読み取り、該画像データに埋め込まれた電子透かしを抽出する段階と、（１０）前記電子透かし検出プログラムが、抽出された前記電子透かしの結果から、前記画像データに改変がなされたかどうかを判断し、改変がなされたと判断した場合、改変の個所を特定する段階と、を有する、画像データ鑑定方法。

【請求項１０】証拠データの改変やすり替えを検知することにより、損害査定の業務プロセスを、安全かつ効率的に行う、保険業務処理システムであって、（１）デジタルデバイスを用いて損害対象物の証拠データを作成する手段と、（２）前記証拠データに改変検出用データを

埋め込み、記憶装置に記録する手段と、（３）前記改変検出用データの埋め込まれた証拠データから、前記改変検出用データを抽出し、該抽出の結果に基づき、証拠データ改変の有無の判断を行い、改変がなされたと判断した場合に改変個所の特定を行うことにより、前記記憶装置に記録された前記証拠データを鑑定する手段と、を有する、保険業務処理システム。

【請求項１１】証拠データの改変やすり替えを検知することにより、損害査定の業務プロセスを、安全かつ効率的に行う、保険業務の実施方法であって、（１）デジタルデバイスを用いて損害対象物の証拠データを作成する段階と、（２）前記証拠データに改変検出用データを埋め込み、記憶装置に記録する段階と、（３）前記改変検出用データの埋め込まれた証拠データから、前記改変検出用データを抽出し、該抽出の結果に基づき、証拠データ改変の有無の判断を行い、改変がなされたと判断した場合に改変個所の特定を行うことにより、前記記憶装置に記録された前記証拠データを鑑定する段階と、を有する、保険業務の実施方法。

【請求項１２】所有者の証明を行うスマートカードであって、（１）所有者の名前またはカード番号が記載されたカード面と、（２）改変個所特定を行う改変検出用データが埋め込まれた所有者の証明データを記憶した記憶装置と、を有する、スマートカード。

【請求項１３】スマートカードに記憶されたデータを読み取るスマートカード・リーダを有する、証明データ検出装置であって、（１）改変検出用データが埋め込まれた所有者の証明データをスマートカードから読み取る手段と、（２）前記改変検出用データの抽出結果に基づき、前記証明データ改変の有無の判断を行い、改変がなされたと判断した場合に改変個所の特定を行う手段、を有する、証明データ検出装置。

【請求項１４】デジタルデバイスで作成されたコンテンツデータを記憶装置に記録するプログラムを含む、媒体であって、（１）コンテンツデータを記録した記録メディアと認証を行う機能と、（２）前記記録メディアに記録されたコンテンツデータを読み取る機能と、（３）前記コンテンツデータに、改変個所の特定を行う改変検出用データを埋め込み、記憶装置に記録する機能と、をコンピュータに実行させるプログラムを含む媒体。

【請求項１５】記録されたコンテンツデータの改変を鑑定するプログラムを含む媒体であって、（１）改変検出用データの埋め込まれたコンテンツデータから、改変検出用データを抽出する機能と、（２）前記改変検出用データの抽出結果に基づき、コンテンツデータ改変の有無の判断を行い、改変がなされたと判断した場合に改変個所の特定を行う機能と、
をコンピュータに実行させるプログラムを含む媒体。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、デジタルデバイスにより作成された画像、音声などのコンテンツデータに電子透かしを埋め込み、埋め込んだ電子透かしを検出することによりコンテンツデータの鑑定行う装置およびその方法に関し、特にコンテンツデータを証拠物件として扱えるように、デジタルデバイス、記録メディア、複数のプログラム間で、認証を適切に行うことによりセキュリティを高度に保持し、コンテンツデータになされた改変の有無及び改変個所の特定を行うことのできる、コンテンツデータ鑑定装置および方法、該装置および方法を用いた保険業務処理システムに関する発明である。

【０００２】

【従来の技術】従来、画像データの改変を検出する方法としてハッシュ関数を用いる方法が知られている。この方法はあらかじめハッシュ関数等を用いて作成された情報を画像データに付加し、改変判定時に、この情報と、画像データに基づき作成したハッシュ値を比較することにより改変が加えられているか否か判断する方法である。しかしながらこのような方式は、画像データに改変がなされたかどうかを検出することはできても、具体的に、画像データのいずれの部分に改変が加えられているかを判定して示すことはできない。これを克服する発明として、特願平１１－１５８３５８がある。この発明は改変検出のための付加情報をコンテンツデータに電子透かしで埋め込み、この付加情報を検出することによりコンテンツデータになされた改変の位置を特定する方法が記載されている。

【０００３】しかしながら、この方法はコンテンツデータの鑑定のしくみを提供しない。ここで鑑定とは、コンテンツデータ作成時点から、コンテンツデータの改変判定時点までにおいて確実にコンテンツデータが受け渡されてきたか、改変がなされている場合、どの過程において改変された可能性がるか、どこが改変されたかを正確に判定する作業を指す。

【０００４】さらに、従来の方法は、カメラ、録音装置、スキャナ、ビデオカメラなどのデジタルデバイスにより作成されたコンテンツデータを証拠物件として扱えるようにするための、高度なセキュリティ保持のしくみ、あるいはこれらのコンテンツデータを用いたクレームサービスおよび保険業務処理を行うプロセスを提供しない。

【０００５】さらに、従来の方法は、本人証明を行う証明物に改ざんがあるかないかを判断し、その改ざんの個所を特定するための機構を提供しない。

【０００６】さらに、従来の方法は、コンテンツデータを作成するデジタルデバイスの種類に関係しない、統一したコンテンツデータの鑑定方法および鑑定装置を提供しない。

【０００７】

【発明が解決しようとする課題】本発明は、上述した従

来技術の問題点に鑑みてなされたものであり、コンテンツデータ作成時点から、コンテンツデータの改変判定時点までにおいて確実にコンテンツデータが受け渡されてきたか、改変がなされている場合、どの過程において改変された可能性があるか、どこが改変されたかを正確に判定する、コンテンツデータ鑑定装置およびその方法を提供することを目的とする。

【０００８】また別の課題は、コンテンツデータが確実に受け渡されてきたかを証明する、高度なセキュリティ保持のしくみや、そのしくみを用いたクレームサービスおよび保険業務処理を行う方法およびそのシステムを提供することである。

【０００９】また別の課題は、本人証明のための、証明物に改ざんがあるかないかを判断し、その改ざんの個所を特定するための方法およびシステムを提供することである。

【００１０】

【課題を達成するための手段】［コンテンツデータ鑑定装置］デジタルデバイスで作成されたコンテンツデータに改変がなされたかどうかを鑑定する、コンテンツデータ鑑定装置は、（１）コンテンツデータを記録したメディアと認証を行う手段と、（２）前記メディアに記録されたコンテンツデータを読み取る手段と、（３）前記コンテンツデータに、該コンテンツを特定するデータを埋め込む手段と、（４）前記コンテンツを特定するデータの埋め込まれたコンテンツデータから、該コンテンツを特定するデータを抽出する手段と、（５）前記コンテンツを特定するデータの抽出結果に基づき、コンテンツデータ改変の有無の判断を行う手段とを有する。好適には、前記コンテンツデータ改変の有無の判断を行う手段（５）が、コンテンツデータに改変がなされたと判断した場合に、改変個所の特定を行う手段を有する。

【００１１】好適には、前記コンテンツデータを読み取る手段（２）において、前記メディアに記録されたコンテンツデータが、デジタルデバイスと前記メディアとの認証結果を含み、該認証結果を読み取る手段を有する。

【００１２】好適には、前記コンテンツを特定するデータ埋め込む手段（３）が、コンテンツデータに、コンテンツデータの認証履歴情報、作成日、作成者、作成機器、登録日などを含むＩＤ情報を埋め込む手段を有する。

【００１３】［改変検出用データ埋め込み装置］デジタルデバイスで作成されたコンテンツデータに、改変検出用データを埋め込む装置は、（１）コンテンツデータを記録したメディアと認証を行う手段と、（２）前記メディアに保存されたコンテンツデータを読み取る手段と、（３）前記コンテンツデータに、改変個所の特定を行う改変検出用データを埋め込み、記憶する手段とを有する。

【００１４】［コンテンツデータ改変鑑定装置］コンテンツデータ改変鑑定装置は、（１）改変検出用データの埋め込まれたコンテンツデータから、改変検出用データを抽出する手段と、（２）前記改変検出用データの抽出結果に基づき、コンテンツデータ改変の有無の判断を行い、改変がなされたと判断した場合に改変個所の特定を行う手段とを有する。

【００１５】［画像データ鑑定装置］デジタルカメラと、デジタルカメラで作成された画像を記録する記録メディアと、記録メディアにアクセスし画像データを読み取り電子透かしを埋め込む電子透かし埋め込み装置と、画像データに埋め込まれた電子透かしを抽出する電子透かし抽出装置、からなる画像データ鑑定装置は、（１）デジタルカメラで画像データを作成する手段と、（２）デジタルカメラと画像記録メディア間で認証を行う手段と、（３）前記認証が成功した場合、前記画像データを前記画像記録メディアに記録する手段と、（４）前記記録メディアと電子透かし埋め込み装置間で認証を行う手段と、（５）前記認証が成功した場合、前記電子透かし埋め込み装置が、前記記録メディアから前記画像データを読み取る手段と、（６）前記電子透かし埋め込み装置が、前記画像データに、改変判定のためのデータを、複数の前記認証の結果および画像データに関連するＩＤ情報と共に、電子透かしとして埋め込む手段と、（７）前記電子透かし埋め込み装置が、前記電子透かしの埋め込まれた、前記画像データを記憶装置に記録する手段と、（８）電子透かし検出装置が、前記記憶装置に記録された画像データを読み取り、該画像データに埋め込まれた電子透かしを抽出する手段と、（９）前記電子透かし検出装置が、抽出された前記電子透かしの結果から、前記画像データに改変がなされたかどうかを判断し、改変がなされた判断した場合、改変の個所を特定する手段と、を有する。

【００１６】［画像データ鑑定方法］デジタルカメラで作成された画像を鑑定する方法は、（１）デジタルカメラで画像データを作成する段階と、（２）デジタルカメラと画像記録メディア間で認証を行う段階と、（３）前記認証が成功した場合、前記画像データを前記画像記録メディアに記録する段階と、（４）前記記録メディアとデバイスドライバ間で認証を行う段階と、（５）前記認証が成功した場合、前記デバイスドライバと、電子透かしを埋め込む電子透かし埋め込みプログラム間で認証を行う段階と、（６）前記電子透かし埋め込みプログラムが、前記記録メディアから前記画像データを読み取る段階と、（７）前記電子透かし埋め込みプログラムが、前記画像データに、改変判定のためのデータを、複数の前記認証の結果および画像データに関連するＩＤ情報と共に、電子透かしとして埋め込む段階と、（８）前記電子透かし埋め込みプログラムが、前記電子透かしの埋め込まれた、前記画像データを記憶装置に記録する段階と、（９）電子透かし検出プログラムが、前記記憶装置に記

録された画像データを読み取り、該画像データに埋め込まれた電子透かしを抽出する段階と、（１０）前記電子透かし検出プログラムが、抽出された前記電子透かしの結果から、前記画像データに改変がなされたかどうかを判断し、改変がなされたと判断した場合、改変の個所を特定する段階とを有する。

【００１７】［保険業務処理システム］証拠データの改変やすり替えを検知することにより、損害査定の業務プロセスを、安全かつ効率的に行う、保険業務処理システムは、（１）デジタルデバイスを用いて損害対象物の証拠データを作成する手段と、（２）前記証拠データに改変検出用データを埋め込み、記憶装置に記録する手段と、（３）前記改変検出用データの埋め込まれた証拠データから、前記改変検出用データを抽出し、該抽出の結果に基づき、証拠データ改変の有無の判断を行い、改変がなされたと判断した場合に改変個所の特定を行うことにより、前記記憶装置に記録された前記証拠データを鑑定する手段と、を有する。

【００１８】［保険業務の実施方法］証拠データの改変やすり替えを検知することにより、損害査定の業務プロセスを、安全かつ効率的に行う、保険業務の実施方法は、（１）デジタルデバイスを用いて損害対象物の証拠データを作成する段階と、（２）前記証拠データに改変検出用データを埋め込み、記憶装置に記録する段階と、（３）前記改変検出用データの埋め込まれた証拠データから、前記改変検出用データを抽出し、該抽出の結果に基づき、証拠データ改変の有無の判断を行い、改変がなされたと判断した場合に改変個所の特定を行うことにより、前記記憶装置に記録された前記証拠データを鑑定する段階とを有する。

【００１９】［スマートカード］所有者の証明を行うスマートカードは、（１）所有者の名前またはカード番号が記載されたカード面と、（２）改変個所特定を行う改変検出用データが埋め込まれた所有者の証明データを記憶した記憶装置とを有する。

【００２０】［証明データ検出装置］スマートカードに記憶されたデータを読み取るスマートカード・リーダを有する、証明データ検出装置は、（１）改変検出用データが埋め込まれた所有者の証明データをスマートカードから読み取る手段と、（２）前記改変検出用データの抽出結果に基づき、前記証明データ改変の有無の判断を行い、改変がなされたと判断した場合に改変個所の特定を行う手段を有する。

【００２１】［改変検出用データを埋め込むプログラムを含む媒体］デジタルデバイスで作成されたコンテンツデータに改変検出用データを埋め込むプログラムを含む、媒体は、（１）コンテンツデータを記録した記録メディアと認証を行う機能と、（２）前記記録メディアに記録されたコンテンツデータを読み取る機能と、（３）前記コンテンツデータに、改変個所の特定を行う改変検出用データを埋め込み、記憶装置に記録する機能とをコンピュータに実行させるプログラムを含む。

【００２２】［コンテンツデータの改変を鑑定するプログラムを含む媒体］記録されたコンテンツデータの改変を鑑定するプログラムを含む媒体は、（１）改変検出用データの埋め込まれたコンテンツデータから、改変検出用データを抽出する機能と、（２）前記改変検出用データの抽出結果に基づき、コンテンツデータ改変の有無の判断を行い、改変がなされたと判断した場合に改変個所の特定を行う機能とをコンピュータに実行させるプログラムを含む。

【００２３】なお、好適には上記デジタルデバイスは、カメラ、録音装置、スキャナ、もしくはビデオカメラである。またコンテンツデータに改変検出用データを埋め込む手段と、改変検出用データの埋め込まれたコンテンツデータから該改変検出用データを抽出する手段と、改変検出用データの抽出結果に基づき、コンテンツデータ改変の有無の判断、あるいは改変がなされた場合に改変個所の特定を行う手段に関しては、以下の改変判定装置に詳細に記す。

【００２４】［改変判定装置］本発明にかかるコンテンツ改変判定装置は、所定の埋め込みデータを埋め込む対象となるコンテンツデータに前記埋め込みデータを付加する、改変検出用データ埋め込み手段（以降データ付加装置と記す）と、前記所定の埋め込みデータが埋め込まれたコンテンツデータに対して改変が加えられたか否かを判定する判定装置とを有する改変判定装置であって、前記データ付加装置は、前記コンテンツデータの少なくとも一部を複数の第１のブロックに分割するコンテンツデータ分割手段と、分割の結果として得られた前記複数の第１のブロックそれぞれに、所定の第１の埋め込みデータそれぞれを付加し、複数の第２のブロックとする埋め込みデータ付加手段とを有し、前記判定装置は、前記第２のブロックの少なくとも一部それぞれに付加された前記埋め込みデータ（第２の埋め込みデータ）を抽出する埋め込みデータ抽出手段（改変検出用データ抽出手段）と、抽出された前記第２の埋め込みデータに基づいて、前記第２のブロックの少なくとも一部それぞれに改変が加えられたか否かを判定する改変判定手段（改変個所特定手段）とを有する。

【００２５】好適には、画像データに所定の埋め込みデータを付加するデータ付加装置と、前記所定の埋め込みデータが埋め込まれた画像データに対して改変が加えられたか否かを判定する判定装置とを有する改変判定装置であって、前記データ付加装置は、画像データを複数の第１の画像ブロックに分割する画像分割手段と、分割の結果として得られた前記複数の第１の画像ブロックそれぞれに、所定の第１の埋め込みデータそれぞれを付加し、複数の第２の画像ブロックとする埋め込みデータ付加手段とを有し、前記判定装置は、前記第２の画像ブロ

ックそれぞれに付加された埋め込みデータ（第２の埋め込みデータ）を抽出する埋め込みデータ抽出手段と、抽出された前記第２の埋め込みデータに基づいて、前記第２の画像ブロックそれぞれに改変が加えられたか否かを判定する改変判定手段とを有する。

【００２６】好適には、前記画像分割手段は、前記画像データを、それぞれ複数の単位データを含む前記複数の第１の画像ブロックに分割し、前記埋め込みデータ付加手段は、互いに対応する２つ以上の前記第１の画像ブロックそれぞれに含まれ、互いに対応する複数の前記単位データの値の関係が、所定の規則に従って前記第１の埋め込みデータを表すように調整して、前記複数の第１の画像ブロックそれぞれに前記第１の埋め込みデータを付加することにより、前記第２の画像ブロックとする。

【００２７】好適には、前記埋め込みデータ付加手段は、いずれかの前記第２の画像ブロックに対して改変が加えられた場合に、改変が加えられた前記第２の画像ブロックに含まれ、互いに対応する前記複数の単位データの値が、前記所定の規則に従わなくなるように調整する。

【００２８】好適には、前記埋め込みデータ抽出手段は、前記複数の第２の画像ブロックそれぞれから、前記第２の画像ブロックそれぞれに含まれる前記複数の単位データの値の関係が、前記所定の規則に従って表すデータを、前記第２の埋め込みデータとして抽出する。好適には、前記改変判定手段は、埋め込まれた前記第１の埋め込みデータと、抽出された前記第２の埋め込みデータとの比較結果に基づいて、前記第２の画像ブロックそれぞれに改変が加えられたか否かを判定する。好適には、前記第１の画像ブロックおよび前記第２の画像ブロックは、それぞれ前記単位データを含み、画像データを所定の処理ブロックに分割し、空間領域から周波数領域に変換処理することにより得られる複数の変換係数を１組以上、含む変換ブロックである。好適には、前記第１の画像ブロックおよび前記第２の画像ブロックは、それぞれ前記単位データを含み、画像データを所定のＤＣＴブロックに分割し、離散的余弦変換（ＤＣＴ）処理することにより得られる複数のＤＣＴ係数を１組以上、含むＤＣＴブロックである。

【００２９】［改変判定装置の作用］本発明にかかる改変判定装置は、まず、処理の対象となるコンテンツデータを複数の部分に分割する。このコンテンツデータは、例えば、事故現場の音声データあるいは破損車両、器物などの画像データであって、意図的な改変が加えられると証拠として用いることができなくなる。次に、本発明にかかる改変判定装置は、上記分割の結果として得られたコンテンツデータの複数の部分それぞれに、改変の判定に用いられ、埋め込みの際に、他の部分へのデータの埋め込みに影響を与えず、また、改変の検出の際に他の部分からの影響を受けない所定の方式により、埋め込みデータ（いわゆる電子透かし（デジタルウォーターマーク））を埋め込こむ。つまり、埋め込みデータは、コンテンツデータの複数の部分それぞれに、複数の部分それぞれに閉じた形で埋め込まれる。最後に、本発明にかかる改変判定装置は、コンテンツデータの上記複数の部分それぞれに閉じた形で埋め込まれた埋め込みデータを、上記複数の部分それぞれに閉じた処理により検出し、コンテンツデータのいずれの部分に改変が加えられたかを判定する。

【００３０】［以下の説明において用いられる具体例］ここで、本発明にかかる改変判定装置が、画像データを分割し、分割した画像データに電子透かし（埋め込みデータ）を埋め込む方式は、分割した画像データそれぞれに閉じて行うことができる限り、どのようなものであってもよい。しかしながら、説明を明確化する必要があるので、以下、本発明にかかる改変判定装置が、例えば、ＪＰＥＧ方式により圧縮符号化された画像データを、それぞれＤＣＴ係数を複数組ずつ含む複数のセット（画像ブロック）に分割し、これらのセットそれぞれに対して、電子透かしを、セットごとに改変の判定が可能なように埋め込み、画像データが改変されたか否かの判定を、これらのセットごとに行う場合を具体例とする。また、本発明にかかる改変判定装置を、画像データの一部に対して埋め込みデータ（電子透かし）を埋め込み、改変の検出を行うようにしても、あるいは、埋め込みデータを埋め込んだ領域と、改変の検出を行う領域とが一致しないようにしてもよいが、以下、画像データの全部に埋め込みデータを埋め込み、改変を行う場合を具体例とする。また、本発明にかかる改変判定装置による埋め込みデータ（電子透かし）の埋め込みの対象となる上記ＤＣＴ係数として、例えば、カラー画像データの輝度成分（Ｙ）を、８×８画素構成の複数のＤＣＴブロック（マクロブロック）にし、これらのＤＣＴブロックをＤＣＴ処理して得られるＤＣＴ係数が用いられる場合を具体例とする。また、それぞれ複数組のＤＣＴ係数を含むセットを選択する方法としては、例えば、乱数を用いてランダムにＤＣＴ係数を選択してセットにする方法、あるいは、単純に隣り合ったＤＣＴ係数を選択してセットにする方法が考えられるが、以下、特に断らない限り、上記２例の後者の最も単純な場合、つまり、ＤＣＴ係数のセットそれぞれが、単純に隣り合った２つのＤＣＴブロックをＤＣＴ変換して得られる２組の（隣接した２つの）ＤＣＴ係数を含むペアである場合を具体例として以下の説明を進める。

【００３１】［データ付加装置の作用］本発明にかかる改変判定装置において、データ付加手段は、画像データに対して、ＤＣＴ係数のペアごとに改変の判定が可能なように、埋め込みデータ（電子透かし）の埋め込みを行う。

【００３２】［画像分割手段］データ付加手段におい

て、画像分割手段は、例えば、ＪＰＥＧ方式により圧縮符号化された圧縮画像データをハフマン復号処理し、復号処理の結果として得られた画像データの３種類の成分の内、輝度成分（Ｙ）のＤＣＴ係数を受け入れ、隣り合った２組のＤＣＴ係数同士に対応付け、対応付けた２組のＤＣＴ係数から構成されるペア（第１の画像ブロック）とする。

【００３３】［埋め込みデータ付加手段］埋め込みデータ付加手段は、ペア（第１の画像ブロック）それぞれに含まれる２組のＤＣＴ係数の内の１つ以上（単位データ）を、相互に対応付けて取り出す（なお、２組のＤＣＴ係数それぞれから１つ以上取り出されるので、１つのペアからは複数の単位データが選択される）。また、埋め込みデータ付加手段は、例えば、鍵情報を用いて乱数を発生し、発生した乱数を用いて、例えば、９６ビットの埋め込みデータをスクランブル処理する。また、埋め込みデータ付加手段は、ペア（第１の画像ブロック）それぞれと、スクランブルされた埋め込みデータ（第１の埋め込みデータ）の各ビットとを対応付ける。さらに、埋め込みデータ付加手段は、ペア（第１の画像ブロック）に含まれる２組のＤＣＴ係数それぞれから取り出され、これら２組のＤＣＴ係数の間で相互に対応するＤＣＴ係数（単位データ）同士の関係が、所定の規則に従って、これらのＤＣＴ係数が含まれていたペア（第１の画像ブロック）に対応付けられた埋め込みデータのビット（第１の埋め込みデータ）の値（１または０）を表すように、これらのＤＣＴ係数の値を調整することにより、埋め込みデータを埋め込む。なお、ペア（第１の画像ブロック）に含まれる２組のＤＣＴ係数から、ＤＣＴ係数を選択する方法は、例えば、予め設定された固定の対応関係に基づいてＤＣＴ係数を選択する方法であっても、乱数に基づいてランダムにＤＣＴ係数を対応付けて選択する係数であってもよい。なお、以下、説明の明確化のために、特に断らない限り、各ペア（第１の画像ブロック）に含まれる２組のＤＣＴ係数それぞれから、ペアごとに乱数を用いてランダムに、互いに対応する３個ずつ（合計６個）のＤＣＴ係数を選択する場合、つまり、ペアが異なれば、異なった位置からＤＣＴ係数が選択されるが、同じペアに含まれるＤＣＴ係数からは、同じ位置のＤＣＴ係数が選択される場合を具体例にして説明を行う。

【００３４】このように各ペアに、埋め込みデータのビットを埋め込むと、例えば、ハッシュ関数を用いて埋め込みデータを埋め込んだ場合と異なり、あるペアに対して加えられた改変は、そのペア以外に影響を与えない。つまり、このように埋め込みをおこなうと、画像の一部分に対する改変の影響は、画像の他の部分に及ばないので、画像に加えられた改変を、部分ごとに判定することができる。

【００３５】［判定装置の作用］埋め込みデータ（第１の埋め込みデータ）の各ビットが埋め込まれた後に、例えば、画像データの一部を塗りつぶし、写っていた物体が消去されるといった改変が加えられると、改変が加えられた部分のペア（第２の画像ブロック）に含まれ、相互に対応するＤＣＴ係数（単位データ）同士の関係が、上記所定の規則から外れることとなり、その埋め込みデータのビット（第２の埋め込みデータ）は、埋め込まれたときの埋込データのビット（第１の埋め込みデータ）と異なる値を示すことになる。

【００３６】また、例えば、９６ビットの埋め込みデータ（第１の埋め込みデータ）を、１０２４ビット×７６８ビット構成の画像を構成する６１４４組のＤＣＴ係数のペア（第１の画像ブロック）に埋め込むと、埋め込みデータ（第１の埋め込みデータ）の各ビットが６４回ずつ、１つの画像データに埋め込まれることになる。

【００３７】一方、画像データの比較的、小面積の部分に対してのみ、改変が加えられた場合、改変が加えられた部分において、対応する埋め込みデータ（第１の埋め込みデータ）のビットを表さなくなるペアの数は、改変が加えられなかった部分において、対応する埋め込みデータ（第１の埋め込みデータ）のビットを表わしているペアの数よりも少なくなるはずである。

【００３８】従って、改変が加えられた可能性がある画像から埋め込みデータ（第２の埋め込みデータ）を抽出し、抽出した埋め込みデータ（第２の埋め込みデータ）の内、埋め込みデータ（第１の埋め込みデータ）の同じビットに対応する６４個のペア（第２の画像ブロック）それぞれが、上記所定の規則に従って、１，０いずれの値を表しているかの多数決を採ると、多数のペアが表している値を、データ付加装置が付加した埋め込みデータ（第１の埋め込みデータ）の値であると判断することができる。同様に、この多数決の結果、少数となったペア（第２の画像ブロック）の位置に、改変が加えられたと推定することができる。

【００３９】本発明にかかる判定装置は、このような埋め込みデータの性質を利用し、改変が加えられた可能性があるＤＣＴ係数のペア（第２の埋め込みデータ）それぞれから、改変が加えられた結果、埋め込まれた当初とは値が変更されている可能性がある埋め込みデータ（第２の埋め込みデータ）を抽出する。さらに、判定装置は、この抽出結果に基づいて、ＤＣＴ係数のペア（第２の画像ブロック）のいずれに改変が加えられているか、つまり、画像データのいずれの部分に改変が加えられているかを判定する。

【００４０】［埋め込みデータ抽出手段］埋め込みデータ抽出手段は、本発明にかかるデータ付加装置により埋め込みデータ（第１の埋め込みデータ）が埋め込まれた後に改変が加えられた可能性があるペア（第２の画像ブロック）の２組のＤＣＴ係数それぞれに含まれ、相互に対応するＤＣＴ係数（単位データ）が、上記所定の規則

に従って表す値（第２の埋め込みデータ）を抽出する。

【００４１】［改変判定手段］改変判定手段は、埋め込みデータの同じビットに対応する複数のペア（第２の画像ブロック）が、１，０いずれの値を表すかの多数決を採り、多数のペアが表す値を、埋め込み時の埋め込みデータ（第１の埋め込みデータ）と判定し、この埋め込みデータと異なる値を表すペア（第２の画像ブロック）に対して、改変がなされたと判定する。

【００４２】［データ付加装置］本発明にかかるデータ付加装置は、画像データに対して改変が加えられたか否かを判定するために、画像データに所定の埋め込みデータを付加するデータ付加装置であって、前記判定は、前記画像データに含まれる複数の第２の画像ブロックそれぞれに付加された第２の埋め込みデータに基づいて、前記画像ブロックそれぞれに改変が加えられたか否かを判断することにより行われ、前記データ付加装置は、画像データを複数の第１の画像ブロックに分割する画像分割手段と、分割の結果として得られた前記複数の第１の画像ブロックそれぞれに、所定の第１の埋め込みデータそれぞれを付加し、前記複数の第２の画像ブロックとする埋め込みデータ付加手段とを有する。

【００４３】［判定装置］また、本発明にかかる判定装置は、画像データを複数の第１の画像ブロックに分割し、分割の結果として得られた前記第１の画像ブロックそれぞれに、所定の第１の埋め込みデータそれぞれを付加することにより作られた複数の第２の画像ブロックそれぞれに改変が加えられたか否かを判定する判定装置であって、前記第２の画像ブロックそれぞれに付加された埋め込みデータ（第２の埋め込みデータ）を抽出する埋め込みデータ抽出手段と、抽出された前記第２の埋め込みデータに基づいて、前記第２の画像ブロックそれぞれに改変が加えられたか否かを判定する改変判定手段とを有する。

【００４４】［改変判定方法］本発明にかかる改変判定方法は、所定の埋め込みデータを埋め込む対象となるコンテンツデータに前記埋め込みデータを付加し、前記所定の埋め込みデータが埋め込まれたコンテンツデータに対して改変が加えられたか否かを判定するコンテンツ改変判定方法であって、前記コンテンツデータを複数の第１のブロックに分割し、分割の結果として得られた前記複数の第１のブロックそれぞれに、所定の第１の埋め込みデータそれぞれを付加し、複数の第２のブロックとし、前記第２のブロックそれぞれに付加された前記埋め込みデータ（第２の埋め込みデータ）を抽出し、抽出された前記第２の埋め込みデータに基づいて、前記第２のブロックそれぞれに改変が加えられたか否かを判定する。

【００４５】［記録媒体］また、本発明にかかる第１の記録媒体は、画像データに所定の埋め込みデータを付加するデータ付加装置と、前記所定の埋め込みデータが埋め込まれた画像データに対して改変が加えられたか否かを判定する判定装置とを有する改変判定装置において、画像データを複数の第１の画像ブロックに分割する画像分割ステップと、分割の結果として得られた前記複数の第１の画像ブロックそれぞれに、所定の第１の埋め込みデータそれぞれを付加し、複数の第２の画像ブロックとする埋め込みデータ付加ステップと、前記第２の画像ブロックそれぞれに付加された埋め込みデータ（第２の埋め込みデータ）を抽出する埋め込みデータ抽出ステップと、抽出された前記第２の埋め込みデータに基づいて、前記第２の画像ブロックそれぞれに改変が加えられたか否かを判定する改変判定ステップとをコンピュータに実行させるプログラムを記録する。

【００４６】また、本発明にかかる第２の記録媒体は、画像データに対して改変が加えられたか否かを判定するために、画像データに所定の埋め込みデータを付加するデータ付加装置において、前記判定は、前記画像データに含まれる複数の第２の画像ブロックそれぞれに付加された第２の埋め込みデータに基づいて、前記画像ブロックそれぞれに改変が加えられたか否かを判断することにより行われ、画像データを複数の第１の画像ブロックに分割する画像分割ステップと、分割の結果として得られた前記複数の第１の画像ブロックそれぞれに、所定の第１の埋め込みデータそれぞれを付加し、前記複数の第２の画像ブロックとする埋め込みデータ付加ステップとをコンピュータに実行させるプログラムを記録する。

【００４７】また、本発明にかかる第３の記録媒体は、画像データを複数の第１の画像ブロックに分割し、分割の結果として得られた前記第１の画像ブロックそれぞれに、所定の第１の埋め込みデータそれぞれを付加することにより作られた複数の第２の画像ブロックそれぞれに改変が加えられたか否かを判定する判定装置において、前記第２の画像ブロックそれぞれに付加された埋め込みデータ（第２の埋め込みデータ）を抽出する埋め込みデータ抽出ステップと、抽出された前記第２の埋め込みデータに基づいて、前記第２の画像ブロックそれぞれに改変が加えられたか否かを判定する改変判定ステップとをコンピュータに実行させるプログラムを記録する。

【００４８】

【発明の実施の形態】以下、本発明の実施形態を説明する。

【００４９】［改変判定装置１］図１は、本発明にかかる改変判定方法を実現する画像改変判定装置１の構成を示す図である。図１に示すように、画像改変判定装置１は、ＣＲＴ表示装置あるいは液晶表示装置等の表示装置１００、キーボードおよびマウス等を含む入力装置１０２、ディジタルカメラインターフェースＩＦ（カメラＩＦ）１０４、メモリカードインターフェース（メモリカードＩＦ）１０６、ＭＯ装置およびＣＤ装置等の記憶装置１０８、および、メモリ１１２およびマイクロプロセ

ッサ（ＣＰＵ）１１４等を含むコンピュータ本体（ＰＣ本体）１１０から構成され、必要に応じて、さらに通信装置１１６が付加される。つまり、画像改変判定装置１は、一般的なコンピュータに、カメラＩＦ１０４およびメモリカードＩＦ１０６を付加した構成を採る。

【００５０】画像改変判定装置１は、これらの構成部分により、光磁気ディスク（ＭＯ）あるいはコンパクトディスク（ＣＤ）等の記録媒体１２０に記録されて記憶装置１０８に供給される埋込・判定プログラム２（図２を参照して後述する）を、メモリ１１２にロードして実行し、画像データに対する電子透かし（埋め込みデータ）の埋め込み処理および改変（人為的に加えられた改変か、データが壊れる等の事故に起因する改変かを問わない）の判定処理を実行する。

【００５１】つまり、画像改変判定装置１は、ディジタルカメラ１４０が撮影した画像を、例えばＪＰＥＧ方式により圧縮符号化して生成した圧縮画像データを、カメラＩＦ１０４を介して受け入れる。あるいは、画像改変判定装置１は、ディジタルカメラ１４０がメモリカード１４２に記録した圧縮画像データを、メモリカードＩＦ１０６を介して受け入れる。圧縮画像データを受け入れると、画像改変判定装置１は、圧縮画像データに電子透かし（埋め込みデータ）を埋め込み、埋め込んだ電子透かし（埋込データ）を用いて、圧縮画像データのいずれの部分に改変が加えられたかを判定する。

【００５２】［埋込・判定プログラム２］図２は、図１に示した画像改変判定装置１が実行し、本発明にかかる改変判定方法を実現する埋込・判定プログラム２の構成を示す図である。図２に示すように、埋込・判定プログラム２は、埋込・抽出部３、鍵情報データベース（ＤＢ）２２および画像データベース（ＤＢ）２４から構成され、埋込・抽出部３は、埋込データ生成部２０、制御部２６、埋込部３０、抽出部４０およびＯＳ５０から構成される。

【００５３】［ＯＳ５０］ＯＳ５０は、例えば、ウィンドウズ（マイクロソフト社商標）等のオペレーティングシステムソフトウェアであって、埋込・判定プログラム２の各構成部分の実行制御を行う。また、ＯＳ５０は、埋込データ生成部２０に対して、メモリカード１４２のシリアル番号および時刻等、電子透かし（埋込データ）の生成に必要なデータを供給するなど、埋込・判定プログラム２の各構成部分の処理に必要とされるデータを供給する。

【００５４】［制御部２６］制御部２６は、例えば、表示装置１００に操作用のＧＵＩ画像（図示せず）を表示し、表示されたＧＵＩ画像に対するユーザの操作を受け入れ、必要に応じて、受け入れた操作を示す操作データを、埋込・判定プログラム２の各構成部分に供給する。また、制御部２６は、受け入れたユーザの操作に応じて、埋込・判定プログラム２の各構成部分の動作を制御する。

【００５５】［画像ＤＢ２４］画像ＤＢ２４は、埋込部３０が埋め込みデータを埋め込んだ圧縮画像データ（ＪＰＥＧデータ）を記憶装置１０８に挿入された記録媒体１２０、あるいは、メモリカードＩＦ１０６に挿入されたメモリカード１４２に記憶・管理し、記憶・管理した画像データを読み出して抽出部４０に対して出力する。

【００５６】［鍵情報ＤＢ２２］鍵情報ＤＢ２２は、画像ＤＢ２２が管理するＪＰＥＧデータと、埋込部３０が、このＪＰＥＧデータへ埋め込みデータを埋め込む際に、乱数を発生させるために用いる鍵（例えば６４ビットの数値）とを対応付けた鍵情報を記憶装置１０８等に記憶・管理し、記憶・管理した鍵情報を読み出して埋込部３０および抽出部４０に対して出力する。

【００５７】［埋込データ生成部２０］埋込データ生成部２０は、例えば、ＯＳ５０から入力されるメモリのシリアル番号といったデータから、９６ビットの埋め込みデータを生成し、埋込部３０に対して出力する。

【００５８】［埋込部３０］図３は、図２に示した埋込部３０の構成を示す図である。図４は、図３に示したデータ埋込部３２の構成を示す図である。図３および図４に示すように、埋込部３０は、復号部３００、データ埋込部３２および符号化部３０４から構成され、データ埋込部３２は、画像分割部３２０、乱数発生部３２２、位置決め部３２４、スクランブル部３２６および係数操作部３２８から構成される。

【００５９】［埋込部３０の概要］埋込部３０は、これらの構成部分により、まず、カラーの圧縮画像データを構成するクロマ成分Ｃｂ，Ｃｒおよび輝度成分Ｙの１組８画素×８画素構成（１組６４画素）のＤＣＴ係数の内、例えば輝度成分ＹのＤＣＴ係数を、それぞれＤＣＴ係数２組ずつを含む複数のペア（第１の画像ブロック）とする。

【００６０】埋込部３０は、さらに、これらのペアそれぞれに、埋込データ生成部２０が発生した９６ビットの埋込データを、鍵情報ＤＢ２２（図２）から供給された鍵情報を用いて、例えば１６ビットの線形合同法により発生した乱数に基づいてスクランブルしたデータ（第１の埋め込みデータ；以下、記述の簡略化のために、このように「スクランブルされた埋め込みデータ」を、単に「埋め込みデータ」とも記す）の各ビットを埋め込む。

【００６１】［埋込部３０の詳細］図５～図１２をさらに参照して、埋込部３０の処理の詳細を説明する。図５は、ディジタルカメラ１４０（図１）が撮影した非圧縮画像データを例示する図である。図６（Ａ）は、図５に例示した非圧縮画像データの一部を示す図であり、（Ｂ）は、（Ａ）に例示した非圧縮画像データ（部分）に含まれるＤＣＴブロック（マクロブロック）を示す図であり、（Ｃ）は、（Ｂ）に示したＤＣＴブロックそれぞれに含まれる８×８構成の画素を示す図である。

【００６２】なお、本来、ＤＣＴブロックと、８×８構成のＤＣＴ係数とは区別する必要があるが、記述の簡略化のために、以下、特に断らない限り、８×８構成のＤＣＴ係数をＤＣＴブロックとも記し、８×８構成のＤＣＴブロックに含まれる各ＤＣＴ係数を、ＤＣＴ係数と記す。

【００６３】ディジタルカメラ１４０（図１）は、例えば、人物および風景を撮影し、図５に例示した非圧縮カラー画像データを生成し、さらに、ＪＰＥＧ方式により圧縮符号化する。つまり、ディジタルカメラ１４０は、図６（Ａ）～（Ｃ）に例示するように、得られた非圧縮画像データに含まれる輝度成分Ｙおよびクロマ成分Ｃｒ，Ｃｂそれぞれを、それぞれ８×８（６４）個の画素を含むＤＣＴブロック（マクロブロックともいう）に分割し、分割の結果として得られたＤＣＴブロックをＤＣＴ変換し、さらに、ハフマン符号化して、ＪＰＥＧ方式の圧縮画像データを生成し、カメラＩＦ１０４を介して、あるいは、メモリカード１４２およびメモリカードＩＦ１０６を介して、ＰＣ本体１１０（図１）により実行される埋込・判定プログラム２の埋込部３０（図２，３）に対して出力する。

【００６４】図７（Ａ）は、ディジタルカメラ１４０から入力される圧縮画像データを復号部３００がハフマン復号して得られる輝度信号ＹのＤＣＴ係数を示す図であり、（Ｂ）は、（Ａ）に示した輝度信号ＹのＤＣＴ係数の内、それぞれ隣り合う２組を対応付ける方法を示す図であり、（Ｃ）は、（Ｂ）に示した方法により対応付けられたＤＣＴ係数のペアを示す図である。

【００６５】埋込部３０は、まず、入力されたＪＰＥＧ方式の圧縮画像データをハフマン復号して輝度成分Ｙおよびクロマ成分Ｃｒ，ＣｂのＤＣＴブロックを得て、得られたこれらのＤＣＴブロックの内、図７（Ａ）に示す輝度成分Ｙの１２２８８個のＤＣＴブロック（１，１～９６，１２８）を、図７（Ｂ），（Ｃ）に示すように、隣り合う２つ（ブロック１，２）同士で６１４４（１２２８８／２）個のペアにする。埋込部３０は、このようにして得られた６１４４（９６×６４）個のペアそれぞれに、上述のように乱数によりスクランブルされた９６ビットの埋め込みデータの各ビットを、６４回ずつ繰り返し対応付ける。

【００６６】図８は、図２，３に示した埋込部３０が１つのペア（図７（Ａ），（Ｂ））に含まれるＤＣＴブロック（ブロック１，２）それぞれから選択した相互に対応するＤＣＴ係数を例示する図である。なお、図８は、ペアｉ（１≦ｉ≦６１４４）に含まれる２つのＤＣＴブロック（ブロック１，２）それぞれから、同じ位置の３個のＤＣＴ係数（２，３），（３，２），（３，３）が選択された場合を例示する。

【００６７】埋込部３０は、例えば、鍵情報ＤＢ２２（図２）から供給された鍵を用いて上述のように生成した乱数を用いて、図８に示すように、ＤＣＴブロック（ブロック１，２）内の相互に対応する３つのＤＣＴ係数（A_1，A_2，B_1，B_2，C_1，C_2；単位データ）を、ペアごとにランダムに選択する。言い換えると、埋込部３０は、任意の一つのペアに含まれるＤＣＴブロック（ブロック１，２）では、同じ位置のＤＣＴ係数をビットの埋め込みのために選択するが、これと異なるペアのＤＣＴブロックでは、異なる位置のＤＣＴ係数を選択する。

【００６８】図９（Ａ），（Ｂ）は、図８に例示したように選択されたブロック１，２それぞれのＤＣＴ係数を、埋め込みデータのビット（値１）を埋め込むために、ＤＣＴ係数の数値を変更する必要がある場合について例示する図である。図１０は、図８に例示したように選択されたブロック１，２それぞれのＤＣＴ係数を、埋め込みデータのビット（値１）を埋め込むために、ＤＣＴ係数の数値を変更する必要がない場合について例示する図である。

【００６９】埋込部３０は、例えば、図８に例示したように、ペアｉの２つのＤＣＴブロック（ブロック１，２）から選択した相互に対応するＤＣＴ係数（A_1，A_2，B_1，B_2，C_1，C_2）値同士の関係が、図９（Ａ），（Ｂ）および図１０に例示するように、上述のようにペアそれぞれに対応付けられた埋め込みデータのビットの値に応じて、下表１に例示する規則（規則１－１，１－２）に従うように調整することにより、各ペアに、対応する埋め込みデータのビットの値（１，０）を埋め込む。

【００７０】

【表１】表１：ＤＣＴ係数の関係を示す規則：ペアに対応付けられた埋め込みデータのビットの値が１である場合：

$(A_1<;A_2\&;\&;B_1<;B_2\&;\&;C_1<;C_2)$¦¦
$(A_1>;A_2\&;\&;B_1>;B_2\&;\&;C_1<;C_2)$¦¦
$(A_1<;A_2\&;\&;B_1>;B_2\&;\&;C_1>;C_2)$¦¦
$(A_1>;A_2\&;\&;B_1<;B_2\&;\&;C_1>;C_2)$

・・・（規則１－１）

である場合：

ペアに対応付けられた埋め込みデータのビットの値が０

$(A_1<;A_2\&;\&;B_1<;B_2\&;\&;C_1>;C_2)$¦¦
$(A_1>;A_2\&;\&;B_1<;B_2\&;\&;C_1<;C_2)$¦¦
$(A_1<;A_2\&;\&;B_1>;B_2\&;\&;C_1<;C_2)$¦¦

$(A_1>;A_2\&;\&;B_1>;B_2\&;\&;C_1>;C_2)$

・・・（規則１－２）

ただし、上記規則１－１，１－２において、X&;&;Yは、条件X,Yの両方を満たすことを示し、X¦¦Yは、条件X,Yのいずれかを満たすことを示す。

【００７１】例えば、図９（Ａ）に例示するように、ペアｉに対応付けられた埋め込みデータのビットの値が１であり、ペアｉの２つのＤＣＴブロック（ブロック１，２）の相互に対応するＤＣＴ係数（A_1，A_2，B_1，B_2，C_1，C_2）の値が、それぞれ４，４，２，３，５，４である場合、これらのＤＣＴ係数の値の関係は、$A_1=A_2$であるため、上記規則１－１，１－２のいずれをも満たさない。

【００７２】そこで、埋込部３０は、図９（Ｂ）内の数字に丸印を付して例示するように、相互に対応するＤＣＴ係数（A_1，A_2，B_1，B_2，C_1，C_2）同士の値の関係が、上記規則１－１の$(A_1<;A_2\&;\&;B_1<;B_2\&;\&;C_1<;C_2)$の条件を満たすことになるように、$A_2$の値を増やして、値１の埋め込みデータのビットを埋め込む。つまり、例えば、値１のビットを埋め込む場合に、ＤＣＴ係数（A_1，A_2，B_1，B_2，C_1，C_2）同士の値が規則１－１を満たさない場合には、常に、これらのＤＣＴ係数同士の関係が、上記規則１－１の内、$(A_1<;A_2\&;\&;B_1<;B_2\&;\&;C_1<;C_2)$の条件を満たすことになるように、ＤＣＴ係数を調節して、値１の埋め込みデータのビットを埋め込む。

【００７３】また、例えば、図１０に例示するように、ペアｉに対応付けられた埋め込みデータのビットの値が１であり、ペアｉの２つのＤＣＴブロック（ブロック１，２）の相互に対応するＤＣＴ係数（A_1，A_2，B_1，B_2，C_1，C_2）の値が、それぞれ３，５，６，３，５，４である場合、これらのＤＣＴ係数の値の関係は、上記規則１－１の条件$(A_1<;A_2\&;\&;B_1>;B_2\&;\&;C_1>;C_2)$を満たしている。従って、この場合には、埋込部３０は、ペアｉの２つのＤＣＴブロック（ブロック１，２）のＤＣＴ係数（A_1，A_2，B_1，B_2，C_1，C_2）の値を変更しない。

【００７４】図１１は、埋込部３０（図２，３）が、ＤＣＴブロックに対して埋め込みデータを埋め込むために用いられる埋め込みテーブルを例示する図表である。なお、図１１には、埋め込みデータビット欄が現れているが、この欄は、埋め込みデータがスクランブル処理されていることを説明するために示したものであり、実際の処理においては用いられない。ここまで説明した埋込部３０の埋め込み処理を、さらに図１１を参照して説明する。埋込部３０は、１０２４画素×７６８画素構成の画像データ（図５，６（Ａ）～（Ｃ））から得られた１２２８８個のＤＣＴブロックの内、隣り合った２つのＤＣＴブロック同士を対応付けて（図７（Ａ）～（Ｃ）、６１４４個のペアを作る。

【００７５】また、埋込部３０は、埋込データ生成部２０（図２）から供給される９６ビットの埋め込みデータを、鍵情報ＤＢ２２から供給される鍵から作成した乱数でスクランブル処理し、スクランブル処理した９６ビットの埋め込みデータのビットそれぞれの値（１，０）を、下記方法により６４回ずつ６１４４個のペアそれぞれに対応付け、図１１に示すように、埋め込みテーブルの埋め込みデータ割り当て欄に書き込む。

【００７６】［埋め込みデータの対応付け方法］なお、図１１に例示するように、連続した９６ペアごとに、それぞれ異なった順番にスクランブルされた９６ビットの埋め込みデータの各ビットが対応付けられるので、例えば、第５番目のペアと、第１６０番目のペアに、埋め込みデータの第７番目のビット（１）が割り当てられる。以下、同様に、６１４４個のペアを、順番に６４組×９６ペアに分割して得られる各組ごとに異なる順番で、各組に含まれる９６ペアそれぞれに、９６ビットの埋め込みデータの各ビットが対応付けられる。

【００７７】例えば、９６ビットの埋め込みデータの第１～第４ビットはそれぞれ、第１～第９６ペアを含む第１組においては、第１１ペア、第５ペア、第３１ペアおよび第９ペアに対応付けられ、第９７～第１９２ペアを含む第２組においては、第９９ペア、第１２６、第１００ペア、第１５３ペアに対応付けられる（後に図１８に例示）。

【００７８】また、埋込部３０は、上述のように生成された乱数を用いて、図８に例示したように、ペアごとに、２つのＤＣＴブロック（ブロック１，２）からいずれのＤＣＴ係数（A_1，A_2，B_1，B_2，C_1，C_2）を取り出すかを決め、取り出したＤＣＴ係数の値を、埋め込みテーブルのブロック１，２の欄に書き込む。上述のように、埋込部３０が８×８構成のＤＣＴ係数のいずれを取り出すかは、ペアごとに一定ではない。

【００７９】以上の処理が終了すると、埋込部３０は、各ペアのＤＣＴブロック（ブロック１，２）から選択されたＤＣＴ係数（A_1，A_2，B_1，B_2，C_1，C_2）が、上記表１に示した規則１－１，１－２に基づいて、埋め込みテーブルの埋め込みデータ割り当て欄のビットの値を表すように、埋め込みテーブルのブロック１，２の欄に書き込まれたＤＣＴ係数（A_1，A_2，B_1，B_2，C_1，C_2）の値を操作する。

【００８０】埋込部３０は、ここまで説明したように埋め込みデータが埋め込まれた輝度成分ＹのＤＣＴ係数（ＤＣＴブロック）と、クロマ成分Ｃｒ，ＣｂのＤＣＴ係数を、再びハフマン符号化して、ＪＰＥＧ方式により伸長可能な圧縮画像データ（ＪＰＥＧデータ）として、画像ＤＢ２４（図２）に対して出力する。

【００８１】［埋込部３０の構成部分］再び図３，４を参照して、埋込部３０の構成部分を説明する。

【００８２】［復号部３００］復号部３００（図３）は、制御部２６（図２）の制御に従って、カメラＩＦ１０４またはメモリカードＩＦ１０６を介して供給されるＪＰＥＧデータをハフマン復号し、復号の結果として得られる３種類のＤＣＴ係数（ＤＣＴブロック）の内、２種類のクロマ成分Ｃｒ，ＣｂのＤＣＴ係数（ＤＣＴブロック）を、符号化部３０４に対して出力し、輝度成分ＹのＤＣＴ係数（ＤＣＴブロック）を、データ埋込部３２に対して出力する。

【００８３】［データ埋込部３２］データ埋込部３２は、図７～図１１を参照して説明した埋め込みデータの埋め込み処理を行う。以下、図４を参照して、データ埋込部３２の各構成部分を説明する。

【００８４】［画像分割部３２０］画像分割部３２０は、復号部３００から入力される輝度信号ＹのＤＣＴ係数（ＤＣＴブロック；図７（Ａ））を、図７（Ｂ），（Ｃ）に示したペアに分割して、係数操作部３２８に対して出力する。

【００８５】［乱数発生部３２２］乱数発生部３２２は、鍵情報ＤＢ２２（図２）から入力される例えば６４ビットの鍵を用いて、１６ビットの線形合同法により乱数を発生し、発生した乱数ＲＮを位置決め部３２４およびスクランブル部３２６に対して出力する。

【００８６】［位置決め部３２４］位置決め部３２４は、画像分割部３２０が作成したペアそれぞれにおいて、乱数発生部３２２から入力される乱数ＲＮを用いて、２つのＤＣＴブロック（ブロック１，２）のいずれのＤＣＴ係数を選択するか（選択するＤＣＴ係数の位置；図８）を決定し、決定したＤＣＴ係数の位置を示す位置データを係数操作部３２８に対して出力する。

【００８７】［スクランブル部３２６］スクランブル部３２６は、乱数発生部３２２から入力される乱数ＲＮを用いて、埋込データ生成部２０（図２）から入力される９６ビットの埋め込みデータをスクランブル処理する。このスクランブル部３２６のスクランブル処理により、９６ビットを１つの繰り返し単位とし、繰り返し単位ごとに異なった順番で９６ビットの埋め込みデータの全てのビットを含み、この繰り返し単位を６４個含むデータ（スクランブルされた埋め込みデータ、以下、単に埋め込みデータとも記す）を係数操作部３２８に対して出力する。

【００８８】［係数操作部３２８の埋め込みテーブル作成処理］係数操作部３２８は、まず、図１１に示した埋め込みテーブルを作成する。つまり、まず、係数操作部３２８は、位置決め部３２４から入力された位置データに基づいて、各ペアの２つのＤＣＴブロック（ブロック１，２；図７（Ｂ）等）からＤＣＴ係数を取り出し（図８）、埋め込みテーブル（図１１）のブロック１，２の欄に書き込み、さらに、スクランブル部３２６から入力された埋め込みデータを埋め込みテーブルの埋め込みデータの割り当て欄に書き込む。

【００８９】［係数操作部３２８のデータ埋め込み処理］図１２は、図４に示した係数操作部３２８が、ＤＣＴブロックのペアに埋め込みデータを埋め込む処理（Ｓ１０）を示す図である。次に、係数操作部３２８は、ＤＣＴ係数（ＤＣＴブロック）のペアそれぞれに、埋め込みテーブル（図１１）において対応付けられた埋め込みデータのビットを埋め込み、埋め込みデータを埋め込んだ輝度成分のＤＣＴ係数Ｙ’として符号化部３０４（図３）に対して出力する。

【００９０】図１２に示すように、係数操作部３２８は、ステップ１００（Ｓ１００）において、６１４４個のペアを示す変数ｉを１に初期設定する。

【００９１】ステップ１０２（Ｓ１０２）において、係数操作部３２８は、第ｉ番目のペアの操作対象となるＤＣＴ係数（A_1，A_2，B_1，B_2，C_1，C_2）を、埋め込みテーブル（図１１）のブロック１，２欄から、埋め込むビットを、同じく埋め込みテーブルの埋め込みデータ割り当て欄から取り出す。

【００９２】ステップ１０４（Ｓ１０４）において、係数操作部３２８は、Ｓ１０２の処理において取り出した埋め込みビットの値が１であるか否かを判断し、埋め込みビットの値が１である場合にはＳ１０６の処理に進み、０である場合にはＳ１１０の処理に進む。

【００９３】ステップ１０６（Ｓ１０６）において、係数操作部３２８は、操作対象のＤＣＴ係数が、表１に示した規則１－１を満たすか否か、つまり、操作対象のＤＣＴ係数が１を表すか判断し、図１０に例示したように、規則１－１を満たす場合にはＳ１１４の処理に進み、これ以外の場合にはＳ１０８の処理に進む。

【００９４】ステップ１０８（Ｓ１０８）において、係数操作部３２８は、操作対象のＤＣＴ係数が、規則１－１を満たすように操作する。

【００９５】ステップ１１０（Ｓ１１０）において、係数操作部３２８は、操作対象のＤＣＴ係数が、表１に示した規則１－２を満たすか否か、つまり、操作対象のＤＣＴ係数が０を表すか否かを判断し、規則１－２を満たす場合にはＳ１１４の処理に進み、これ以外の場合にはＳ１１２の処理に進む。

【００９６】ステップ１１２（Ｓ１１２）において、係数操作部３２８は、操作対象のＤＣＴ係数が、規則１－２を満たすように操作する。

【００９７】ステップ１１４（Ｓ１１４）において、係数操作部３２８は、変数ｉが６１４４であるか否か、つまり、全てのペアに対して埋め込みデータの埋め込み処理が終了したか否かを判断し、終了した場合には処理を終了し、これ以外の場合には変数ｉを１増やしてＳ１０２の処理に戻る。

【００９８】［符号化部３０４］符号化部３０４（図３）は、復号部３００から入力されたクロマ成分Ｃｒ，

ＣｂのＤＣＴ係数と、データ埋込部３２から入力され、埋め込みデータが埋め込まれた輝度成分ＹのＤＣＴ係数Ｙ’とをハフマン符号化し、画像ＤＢ２２に対して出力する。

【００９９】［抽出部４０］図１３は、図２に示した抽出部４０の構成を示す図である。図１４は、図１３に示した埋め込みデータ抽出部４２の構成を示す図である。図１３および図１４に示すように、抽出部４０は、復号部４００、画像分割部４０２、符号化部４０４、画像合成部４０６、埋込データ抽出部４２、改変検出部４４およびクラスタリング部４６から構成され、埋込データ抽出部４２は、乱数生成部４２０、位置決め部４２２，抽出順序生成部４２４、対応付け部４２６およびデータ抽出部４２８から構成される。

【０１００】［抽出部４０の概要］埋込部３０により、図７～図１２を参照して上述したように埋め込みデータが埋め込まれたＪＰＥＧデータの一部または全部に対して、その後、改変が加えられると、各ペアの２つのＤＣＴブロック（ブロック１，２；図７（Ｂ）等）の間で相互に対応し、埋め込みデータの埋め込みに用いられたＤＣＴ係数（A_1，A_2，B_1，B_2，C_1，C_2；図８等）の値の関係が、上記表１に示した規則１－１，１－２に従って、図９（Ａ），（Ｂ）および図１０に例示した処理により埋め込まれたビットの値を示さなくなる。

【０１０１】抽出部４０は、上述した構成部分により、埋め込みデータが埋め込まれたＪＰＥＧデータのこのような性質を利用して、埋込部３０が生成したＪＰＥＧデータに改変が加えられたか否か、および、改変が加えられた場合には、画像データ（図５）のいずれの部分に改変が加えられたかを判定し、表示する。

【０１０２】［抽出部４０の詳細］以下、図１５～図２２をさらに参照して、抽出部４０の処理を詳細に説明する。上述したように、埋込部３０（図２，３）においては、各ペアにおいて、埋め込みデータの埋め込みに用いられるＤＣＴ係数の位置は、同じく、鍵情報ＤＢ２２から供給された鍵から生成された乱数によって求められる。従って、抽出部４０においても、埋込部３０と同じ鍵を使うことにより、各ペアのＤＣＴブロック（ブロック１，２；図８）において、いずれのＤＣＴ係数が、埋め込みデータの埋め込みに用いられたかを知ることができる。

【０１０３】また、埋込部３０においては、９６ビットの埋め込みデータの各ビットは、鍵情報ＤＢ２２から供給される鍵から生成された乱数によってスクランブルされ、各ペアに対応付けられている。従って、抽出部４０においても、埋込部３０と同じ鍵を使うことにより、いずれのペアに、９６ビットの埋め込みデータのいずれのビットが対応付けられたかを知ることができる。

【０１０４】抽出部４０は、このように、埋込部３０と同じ鍵を用いて、各ペアの２つのＤＣＴブロック（ブロック１，２）において、いずれのＤＣＴ係数がビットの埋め込みに用いられたかを知り、さらに、ビットの埋め込みに用いられた相互いに対応するＤＣＴ係数同士の値の関係が、上記表１に示した規則１－１，１－２のいずれに該当するかによって、各ペアに埋め込まれた埋め込みデータのビットの値（１，０）を抽出する。次に、抽出部４０は、埋込部３０と同じ鍵を用いて、各ペアから抽出された埋め込みデータのビットの値が、埋め込みデータのいずれのビットに対応するかを判定する。

【０１０５】図１５（Ａ）は、埋込部３０（図２，３）が埋め込みデータを埋め込んだＪＰＥＧデータを伸長した画像を例示する図であり、（Ｂ）は、（Ａ）に示した画像のなかで改変を行う個所の例示であり、（Ｃ）は、改変後の画像を例示する図である。ここで、例えば、埋込部３０が、図５および図６（Ａ）～（Ｃ）に示した画像データから得られたＪＰＥＧデータに対して、図７～図１２に示したように埋め込みデータを埋め込んで生成したＪＰＥＧデータを、誰かが伸長し、図１５（Ａ）に例示する画像を得て、図１５（Ｂ）に点線で示す個所に改変を加え、図１５（Ｃ）に示すように、画像中の車の部分消去／修正した画像を生成し、再度、ＪＰＥＧ方式で圧縮符号化し、元のＪＰＥＧデータと置き換えたとすると、改変は画像のごく一部に加えられたため、埋め込みデータの同一のビットに対応付けられた６４個のペアから抽出された６４の値の多くは、改変前の値を示し、少数だけが改変によって変更された値を示すはずである。

【０１０６】抽出部４０は、画像の一部に変更が加えられた場合のこのような性質を利用して、各ペアから抽出したビットを、埋め込みデータの各ビットに対応付けて多数決を採り、埋め込みデータの第ｋビットに対応する６４個のペアの多数から値１（０）が抽出され、少数のペアから値０（１）が抽出された場合には、埋込部３０が、これら６４個のペアに、第ｋビットとして、値１（０）を埋め込んだと推定する。つまり、抽出部４０は、埋め込みデータの各ビットについて、抽出された値の多数決を採り、埋込部３０が各ペアに埋め込んだ埋め込みデータのビットの値を推定するとともに、多数決の結果、少数となった値が抽出されたペアに対して、改変が加えられたと判定する。

【０１０７】図１６は、改変が加えられた部分を示す２値画像を、元の画像と合成して示す画像を例示する図である。さらに、抽出部４０は、例えば、図１６に示すように、改変が加えられたペアを示す２値画像（図１６の中央付近とナンバープレート部の網掛け部分）と、図５に示した元の画像とを合成して、いずれの部分に改変が加えられたかを表示装置１００（図１）等に表示する。

【０１０８】図１７は、クラスタリング処理により、改変が加えられた範囲を示す画像を、元の画像と合成して示す画像を例示する図である。あるいは、抽出部４０

は、例えば、図１７に示すように、クラスタリング処理により、図１６に示した２値画像のモザイク状の部分が存在する範囲を示す画像（図１７左上の長方形）を得て、この画像と、図５に示した元の画像とを合成して、いずれの範囲に改変が加えられたかを表示装置１００等に表示する。

【０１０９】このような処理を行うために、まず、抽出部４０は、画像ＤＢ２２から供給されるＪＰＥＧデータをハフマン復号し、得られた３種類のＤＣＴ係数（ＤＣＴブロック）の内、輝度成分Ｙの１２２８８個のＤＣＴ係数（ＤＣＴブロックＹ’）を取り出し、隣り合ったＤＣＴ同士を、図７（Ｂ），（Ｃ）に示したように、６１４４個のペアにする。

【０１１０】抽出部４０は、これらのペアそれぞれに含まれる２つのＤＣＴブロック（ブロック１，２；図８）の埋め込みデータの埋め込みに用いられたＤＣＴ係数の関係が、上記表１に示した規則１－１，１－２のいずれに該当するかを判断し、各ペアに埋め込まれた埋め込みデータ（第２の埋め込みデータ）のビットの値（１，０）を抽出する。もし、２つのＤＣＴブロック（ＤＣＴブロック１，２）の対応するＤＣＴ係数が等しい場合（例えば、$A_1 = A_2$）には、この関係は規則１－１，１－２のいずれにも当てはまらないため、抽出部４０は、直ちにこのペアに改変が加えられたと判断することができる。なお、以下、説明の明確化のために、対応するＤＣＴ係数が等しくない場合を具体例とする。

【０１１１】図１８は、埋込部３０（図２，３）が生成したＪＰＥＧデータに、改変・誤りが加えられていない場合に、抽出部４０が改変等がなされていないＪＰＥＧデータに含まれる各ペアから抽出するビットの値を示す図である。抽出部４０が、埋込部３０が生成した後、改変も誤りも加えられていないＪＰＥＧデータに含まれる各ペア（第２の画像ブロック）から抽出した埋め込みデータのビットの値を、図１８に示すように、各ペアに、埋め込みデータのいずれのビットが対応付けられているかに従って並べると、各埋め込みデータに対応するペアから抽出された全てのビットの値は一致する。

【０１１２】図１９は、埋込部３０（図２，３）が生成したＪＰＥＧデータに、改変・誤りが加えられた場合に、抽出部４０が改変等がなされたＪＰＥＧデータに含まれる各ペアから抽出するビットの値を例示する図である。一方、例えば、抽出部４０が、埋込部３０が生成した後、改変等が加えられたＪＰＥＧデータに含まれる各ペア（第２の画像ブロック）から抽出した埋め込みデータのビットの値を、図１８と同様に、各ペアに、埋め込みデータのいずれのビットが対応付けられているかに従って並べると、図１９に示すように、改変が加えられた部分の少数のペアから抽出されたビットは、図１９中に太枠を付した値として示すように、改変が加えられていない他の多数のペアから抽出されたビットと異なる値を採り、不整合を生じる。抽出部４０は、このようにして多数決により得られたビットの値を、埋込部３０が埋め込んだ埋め込みデータのビットの値と推定する。

【０１１３】図２０は、抽出部４０（図１３，１４）が、図１５に例示したように改変が加えられたＪＰＥＧデータから、図１９に例示したように改変等が加えられたペアを判定し、改変が加えられたペアの画像内における位置を示す２値画像を例示する図である。なお、説明の都合上、図２０に示した例と、図１５等に示した例とは、必ずしも一致しない。このように、抽出部４０は、図２０に例示するように、多数決により推定された値と異なる値のビットが抽出されたペアが、画面内のいずれに位置するかを示す２値画像を生成する。なお、抽出部４０が生成した２値画像は、図１６を参照して上述したように、元の画像と合成され、表示装置１００（図１）等に表示される。

【０１１４】図２１（Ａ）～（Ｄ）は、抽出部４０（図１３，１４）が、図１５に例示したように改変が加えられたＪＰＥＧデータから、図１９に例示したように改変等が加えられたペアを判定し、改変が加えられたペアが画像内において、いずれの範囲に存在するかを示すクラスタリング画像を例示する図である。なお、説明の都合上、図２１（Ａ）～（Ｄ）に示した例と、図１５等に示した例とは、必ずしも一致しない。また、抽出部４０は、図２１（Ａ），（Ｃ）にそれぞれ例示するように、多数決により推定された値と異なる値のビットが抽出されたペアが、画面内のいずれの範囲に存在するかを判定し、それぞれ図２１（Ｂ），（Ｄ）に例示するクラスタリング画像を生成する。なお、抽出部４０が生成したクラスタリング画像は、図１７を参照して上述したように、元の画像と合成され、表示装置１００（図１）等に表示される。

【０１１５】［抽出部４０の構成部分］以下、再び図１３，１４を参照して、抽出部４０の各構成部分を説明する。

【０１１６】［復号部４００］復号部４００は、操作に応じた制御部２６の制御に従って、画像ＤＢ２２から供給されるＪＰＥＧデータをハフマン復号し、復号の結果として得られた３種類の画像成分の内、クロマ成分Ｃｒ，Ｃｂを符号化部４０４に対して出力し、輝度成分Ｙ’を、画像分割部４０２に対して出力する。

【０１１７】［画像分割部４０２］画像分割部４０２は、復号部４００から入力された輝度成分Ｙ’を、ＤＣＴ係数（ＤＣＴブロック）単位に分割し、分割の結果として得られたＤＣＴ係数（ＤＣＴブロック）を、埋込データ抽出部４２に対して出力する。

【０１１８】［埋込データ抽出部４２］埋込データ抽出部４２は、画像分割部４０２から入力された輝度成分Ｙ’のＤＣＴブロックを２つずつ対応付けて、埋込部３０においてと同様なペア（図７（Ｂ），（Ｃ）および図

8等）とし、これらのペアに埋め込まれた埋め込みデータのビットの値を抽出し、図18，19に例示した形式の抽出データとして改変検出部44に対して出力する。また、埋込データ抽出部42は、画像分割部402から入力された輝度成分Y'をそのまま、輝度成分Yとして符号化部404に対して出力する。

【0119】［対応付部426］対応付部426（図14）は、画像分割部402から入力された12288個のDCT係数（DCTブロック）の内、隣り合った2つのDCTブロック（ブロック1，2；図7（B）等）同士を対応付け、6144個のDCT係数のペア（図7（B），（C））を生成し、データ抽出部428に対して出力する。つまり、対応付部426は、埋込部30（図2，3）の画像分割部320（図4）に対応し、画像分割部320と同様に、DCTブロックのペアを生成する。

【0120】［乱数発生部420］乱数発生部420は、鍵情報DB22（図2）から供給され、埋込部30が埋め込みデータの埋め込みに用いた鍵と同じ鍵を用いて、埋込部30においてと同じ方法により乱数RNを発生し、発生した乱数RNを、位置決め部422および抽出順序生成部424に対して出力する。つまり、乱数発生部420は、埋込部30の乱数発生部322（図4）に対応し、乱数発生部322が用いる鍵と同一の鍵から、乱数発生部322と同一方法で同一の乱数を生成する。

【0121】［位置決め部422］位置決め部422は、乱数発生部420から入力された乱数RNから、ペアそれぞれに含まれる2つのDCTブロック（ブロック1，2）のいずれのDCT係数が、埋込部30において埋め込みデータの埋め込みに用いられたかを示す位置データを生成し、データ抽出部428に対して出力する。つまり、位置決め部422は、埋込部30の位置決め部324に対応し、位置決め部324が用いた乱数と同一の乱数から、位置決め部324と同一の位置データを生成する。

【0122】［抽出順序生成部424］上述したように、対応付部426からデータ抽出部428に入力される6144個のペアは、96個のペアを1組として、各組ごとに異なる順番で、各組に含まれる96個のペアそれぞれに、96ビットの埋め込みデータのビットそれぞれが対応付けられている。抽出順序生成部424は、乱数発生部420から入力された乱数RNから、いずれのペアに、96ビットの埋め込みデータのいずれの順番のビットが対応付けられたかを示す順序データを生成し、データ抽出部428に対して出力する。

【0123】データ抽出部428は、対応付部426から入力されるペアそれぞれに含まれる2つのDCTブロック（ブロック1，2）において、位置決め部422から入力される位置データが示す相互に対応するDCT係数（図8等）同士の値の関係が、上記表1に示した規則1－1，1－2のいずれと一致するかを判定し、各ペアに埋め込まれた埋め込みデータのビットの値を抽出する。さらに、データ抽出部428は、抽出したビットの値を、抽出順序生成部424から入力される順序に従って並び替え、図18，19に例示した形式の抽出データを生成し、抽出順序生成部424に対して出力する。

【0124】データ抽出部428のビット抽出処理を、図22を参照してさらに説明する。図22は、図14に示したデータ抽出部428が、各ペアに埋め込まれた埋め込みデータのビットを抽出する処理を示すフローチャートである。図22に示すように、ステップ120（S120）において、データ抽出部428は、6144個のペアを示す変数iに1を代入し、初期設定を行う。

【0125】ステップ122（S122）において、データ抽出部428は、変数iが示す第i番目のペアを抽出対象として取り出す。

【0126】ステップ124（S124）において、データ抽出部428は、取り出した抽出対象のペアに含まれる2つのDCTブロック（ブロック1，2）において、位置決め部422から入力される位置データが示すDCT係数の関係が、上記表1に示した規則1－1，1－2のいずれに当てはまるかを判定し、規則1－1に当てはまる場合には、第i番目のペアから値1のビットを抽出し、規則1－2に当てはまる場合には、値0のビットを抽出する。さらに、データ抽出部428は、抽出順序生成部424から入力される順序データに基づいて、抽出したビットの値が、埋め込みデータのいずれのビットに対応するかを判定し、抽出データ（図18，19）中の判定の結果として得られた位置に、抽出したビットの値（1，0）を書き込む。

【0127】ステップ126（S126）において、データ抽出部428は、変数iが6144であるか否か、つまり、全てのペアからのビットの抽出が終了したか否かを判断し、終了した場合には処理を終了し、これ以外の場合には変数iを1増やしてS122の処理に進む。

【0128】全てのペアからビットの抽出が完了すると、データ抽出部428は、図18，19に例示した抽出データにおいて、96ビットの埋め込みデータのビットそれぞれに対応して抽出された64個の値の多数決を採り、埋込部30（図2，3）において埋め込まれた埋め込みデータを推定し、各ペアを輝度成分Yとして符号化部404に対して出力する。

【0129】［符号化部404］符号化部404（図13）は、復号部400から入力されたクロマ成分Cr，Cbおよび符号化部404から入力された輝度成分Yをハフマン符号化して、JPEGデータを生成し、画像合成部406に対して出力する。

【0130】［改変検出部44］改変検出部44は、データ抽出部428から入力された抽出データ（図18，

１９）から、図２０に示した２値画像を生成し、画像合成部４０６に対して出力する。

【０１３１】［クラスタリング部４６］クラスタリング部４６は、改変検出部４４から入力された２値画像において、改変等がなされたことが示されている範囲を示すクラスタリング画像（図２１）を生成し、画像合成部４０６に対して出力する。

【０１３２】［画像合成部４０６］画像合成部４０６は、操作入力に応じた制御部２６の制御に従って、符号化部４０４から入力されるＪＰＥＧデータを伸長し、図５あるいは図１５（Ｃ）等に例示した画像を生成し、生成した画像をそのまま表示装置１００（図１）に表示する。あるいは、画像合成部４０６は、改変検出部４４から入力された２値画像、あるいは、クラスタリング部４６から入力されたクラスタリング画像と、伸長の結果として得られた画像とを合成し、図１６あるいは図１７に例示した画像を生成し、画像中において改変等がなされた部分を表示装置１００に表示する。あるいは、画像合成部４０６は、改変検出部４４から入力された２値画像、あるいは、クラスタリング部４６から入力されたクラスタリング画像を、そのまま表示装置１００に表示して、画像中のいずれの範囲に改変等がなされたかを示す。

【０１３３】［画像改変判定装置１の埋め込みデータ埋め込み処理］以下、図２３を参照して、画像改変判定装置１による埋め込みデータの埋め込み処理を、全体を通して説明する。図２３は、図１に示した画像改変判定装置１による埋め込みデータの埋め込み処理（Ｓ２０）を示すフローチャートである。

【０１３４】ステップ２００（Ｓ２００）において、復号部３００（図３）は、カメラＩＦ１０４等を介して供給されるＪＰＥＧデータをハフマン復号し、輝度成分Ｙの１２２８８個のＤＣＴ係数（ＤＣＴブロック）を、データ埋込部３２に対して出力する。画像分割部３２０は、入力されたＤＣＴ係数（ＤＣＴブロック；図７（Ａ））を、６１４４個のペア（図７（Ｂ），（Ｃ））に分割して、係数操作部３２８に対して出力する。乱数発生部３２２は、鍵情報ＤＢ２２（図２）から入力される鍵を用いて乱数を発生し、発生した乱数ＲＮを位置決め部３２４およびスクランブル部３２６に対して出力する。

【０１３５】位置決め部３２４は、乱数発生部３２２から入力される乱数ＲＮを用いて、埋め込みデータの埋め込みに用いられるＤＣＴ係数の位置を示す位置データを生成し、係数操作部３２８に対して出力する。スクランブル部３２６は、乱数発生部３２２から入力される乱数ＲＮを用いて、埋込データ生成部２０（図２）から入力される９６ビットの埋め込みデータをスクランブル処理し、係数操作部３２８に対して出力する。

【０１３６】ステップ１２（Ｓ１２）において、まず、係数操作部３２８（図４）は、各ペアにおいて、埋め込みデータを埋め込むための操作の対象となるＤＣＴ係数（A_1，A_2，B_1，B_2，C_1，C_2；図8等）を、位置決め部３２４から入力される位置データに基づいて選択する。さらに、係数操作部３２８は、各ペアを、スクランブル部３２６から入力される埋め込みデータの各ビットと対応付け、図１１に示した埋め込みテーブルを作成する。さらに、係数操作部３２８は、埋め込みテーブルから操作の対象となるＤＣＴ係数と、埋め込むビットとを順次、取り出し、上記表１に示した規則１－１，１－２に従って、図９（Ａ），（Ｂ）および図１０に例示したように、各ペアに埋め込みデータの各ビットを埋め込む。

【０１３７】全てのペアへのビットの埋め込みが終了すると、ステップ２０２（Ｓ２０２）において、符号化部３０４（図３）は、埋め込みデータが埋め込まれた輝度成分のＤＣＴ係数（ＤＣＴブロック）と、復号部３００から入力されるその他の成分のＤＣＴ係数とをハフマン符号化し、ＪＰＥＧデータを生成して画像ＤＢ２２（図２）に対して出力する。画像ＤＢ２２は、埋込部３０から入力されたＪＰＥＧデータを記憶・管理する。

【０１３８】［画像改変判定装置１の埋め込みデータ抽出処理］以下、図２４を参照して、画像改変判定装置１による埋め込みデータの抽出処理を、全体を通して説明する。図２４は、図１に示した画像改変判定装置１による埋め込みデータの抽出処理（Ｓ２２）を示すフローチャートである。

【０１３９】ステップ２２０（Ｓ２２０）において、復号部４００（図１３）は、画像ＤＢ２２から供給されるＪＰＥＧデータをハフマン復号し、輝度成分Ｙ’を、画像分割部４０２に対して出力する。画像分割部４０２は、輝度成分Ｙ’を１２２８８個のＤＣＴ係数（ＤＣＴブロック）に分割して、埋込データ抽出部４２に対して出力する。埋込データ抽出部４２において、対応付部４２６は、隣り合ったＤＣＴ係数（ＤＣＴブロック；図７（Ａ））を２つずつ対応付けて、６１４４個のペア（図７（Ｂ），（Ｃ））を作成し、データ抽出部４２８に対して出力する。乱数発生部４２０（図１４）は、鍵情報ＤＢ２２（図２）から入力される鍵を用いて乱数を発生し、発生した乱数ＲＮを位置決め部４２２および抽出順序生成部４２４に対して出力する。

【０１４０】位置決め部４２２は、乱数発生部４２０から入力される乱数ＲＮを用いて、埋め込みデータの埋め込みに用いられるＤＣＴ係数の位置を示す位置データを生成し、データ抽出部４２８に対して出力する。抽出順序生成部４２４は、乱数発生部３２２から入力される乱数ＲＮを用いて、各ペアに、いずれの埋め込みデータのビットが対応付けられているかを示す順序データを生成し、データ抽出部４２８に対して出力する。

【０１４１】ステップ１２（Ｓ１２）において、図２２

に示したように、データ抽出部４２８は、ペアを順次、取り出して抽出対象とし、位置決め部４２２から入力される位置データが示す２つのＤＣＴブロック（ブロック１，２）のＤＣＴ係数の値の関係が、上記表１に示した規則１－１，１－２のいずれに当てはまるかに応じて、各ペアに埋め込まれたビットの値を抽出する。さらに、データ抽出部４２８は、抽出順序生成部４２４から入力される順序データに基づいて、抽出したビットの値が、埋め込みデータのいずれのビットに対応するかを判定し、抽出データ（図１８，１９）中の判定の結果として得られた位置に、抽出したビットの値（１，０）を書き込む。

【０１４２】全てのペアからのビットの値の抽出が終了すると、ステップ２２２（Ｓ２２２）において、データ抽出部４２８は、図１８，１９に例示した抽出データにおいて、９６ビットの埋め込みデータのビットそれぞれに対応して抽出された６４個の値の多数決を採り、埋込部３０（図２，３）において埋め込まれた埋め込みデータを推定する。さらに、符号化部４０４（図１３）は、復号部４００から入力されたクロマ成分Ｃｒ，Ｃｂおよび符号化部４０４から入力された輝度成分Ｙをハフマン符号化して、ＪＰＥＧデータを生成し、画像合成部４０６に対して出力する。

【０１４３】ステップ２２４（Ｓ２２４）において、改変検出部４４は、データ抽出部４２８から入力された抽出データ（図１８，１９）から、図２０に示した２値画像を生成し、画像合成部４０６に対して出力する。クラスタリング部４６は、改変検出部４４から入力された２値画像において、改変等がなされたことが示されている範囲を示すクラスタリング画像（図２１）を生成し、画像合成部４０６に対して出力する。画像合成部４０６は、操作入力に応じた制御部２６の制御に従って、例えば、改変検出部４４から入力された２値画像、あるいは、クラスタリング部４６から入力されたクラスタリング画像と、伸長の結果として得られた画像とを合成し、図１６あるいは図１７に例示した画像を生成し、画像中において改変等がなされた部分を表示装置１００に表示する。

【０１４４】［変形例］以下、本発明の実施形態の変形例を説明する。

【０１４５】［画像データの領域］ここまで説明した実施形態においては、画像データの全領域をペアに分割し、画像データの全領域に対して改変の判定を行う場合を具体例としたが、画像データの分割および改変の判定は、画像データの一部の領域に対して行っても、分割した領域と改変を判定する領域とが一致しなくてもよい。

【０１４６】［ＤＣＴ以外の変換方式］また、実施形態においては、画像データの圧縮符号化のためにＤＣＴ処理を行う場合について説明したが、本発明にかかる改変判定方法は、ＤＣＴ処理ではなく、例えばウェーブレット変換、フーリエ変換およびＦＦＴ（高速フーリエ変換）といった、空間領域のデータを周波数領域のデータに変換する空間・周波数変換を用いて画像データを圧縮符号化する場合にも、ほとんど変更なしに応用することができる。

【０１４７】［輝度成分以外への埋め込み］また、実施形態においては、輝度成分ＹのＤＣＴ係数に埋め込みデータを埋め込む場合を説明したが、本発明にかかる改変判定方法は、クロマ成分Ｃｒ，Ｃｂに埋込データを埋め込む場合にも応用可能である。また、本発明にかかる改変判定方法は、ＲＧＢ画像データ等、他の形式の画像データに対して適用できることは言うまでもない。

【０１４８】［ＤＣＴブロックの対応付け］また、実施形態においては、ＤＣＴブロックの対応付けを、隣接した２つのＤＣＴブロック同士を対応付けることにより行ったが、例えば、乱数を用いて、１２２８８個のＤＣＴブロックの２つをランダムに選択し、対応付けしてペアとしてもよい。また、図４に点線で示したように、乱数発生部３２２から画像分割部３２０に乱数ＲＮを供給し、画像分割部３２０が、この乱数ＲＮを用いて、ランダムに２つずつＤＣＴ係数（ＤＣＴブロック）を選択してペアを作成するようにしてもよい。

【０１４９】また、図１４に点線で示したように、乱数発生部４２０から対応付部４２６に乱数ＲＮを供給し、対応付部４２６が、この乱数ＲＮを用いて、画像分割部３２０が対応付けたペアを再現するようにしてもよい。また、埋込データのスクランブル方法は、実施形態として示した方法に限定されず、埋込データの各ビットが、総ペアに対して定数回ずつ割り当てられるような方法であればよい。

【０１５０】［画像データ以外への適用］また、本発明にかかる埋込・判定プログラム２を適切に変形することにより、画像データの他、音声データ等、他の種類のコンテンツデータのいずれの部分に改変が加えられたかを判定する用途に応用することができる。

【０１５１】音声データに対して本発明を応用する場合を例としてさらに説明する。音声データは、連続するサンプル点を１ブロックとして処理することができ、例えば、サンプリング周波数４４．１ｋＨｚの音声データ、１０２４個ずつを１つのブロックとすれば、１秒分の音声データには、４４個の音声データブロックが含まれることになる。これらの音声データブロックをＦＦＴなどにより周波数領域のデータブロックに変換すると、実施形態と同様な方法により埋込データを埋め込むことができ、埋め込んだデータを用いて改変を検出することができる。

【０１５２】［複数の改変判定装置１の接続方法］図２５は、それぞれ画像ＤＢ２４（２４－１～２４－ｎ）を有する複数の画像改変判定装置１（１－１～１－ｎ）を接続した改変判定システム４の構成を示す図である。な

お、図２５に示すように、それぞれ画像ＤＢ２４（２４－１～２４－ｎ）および埋込・抽出部３（３－１～３－ｎ）を１つずつ含む複数の画像改変判定装置１－１～１－ｎを、通信装置１１６（図１；図２５において図示せず）を介して接続して、各画像改変判定装置１－１～１－ｎで画像データに加えられた改変を検出する場合には、各画像ＤＢ２４－１～２４－ｎにおいて記憶・管理される画像データと、その鍵とを、画像改変判定装置１－１の鍵情報ＤＢ２２－１により一元管理し、各画像改変判定装置１－１～１－ｎに対して鍵を配送するようにすると、高いセキュリティを確保することができる。

【０１５３】［コンテンツデータ鑑定装置］次に、上記改変判定装置を用いて、デジタルデバイスにより作成されたコンテンツデータを証拠物件として扱えるようにするための、高度なセキュリティ保持のしくみに取り入れた、コンテンツデータ鑑定装置の実施例を示す。なお以下で使用する、タンパープルーフ（TamperProof）の技術については、機密性の高いアルゴリズムが含まれるソフトウエア／ハードウエア・モジュールを逆アセンブラ等のリバース・エンジニアリングから守るための周知技術である。またＲＣ４とはRon Rivest（RSADataSecurity Inc.）が作った暗号化アルゴリズムであり周知技術である。その暗号化のアルゴリズムについての説明は省力する。図２６に本発明のデータ鑑定装置のブロック図を示す。デジタルカメラ５１０で生成されたJPEG画像が、改ざん／すり替え等によりオリジナリティーが毀損されることなくPC上デバイスドライバ・プログラム５３０（以降単にドライバと呼ぶ）を経て記憶装置（ハードディスクなど）に保存出来る。またPC上のアプリケーション５５０によりJPEG画像のオリジナリティーを検査し、その結果を表示する。加えて、JPEG画像が改ざんされていた場合は、その改ざん場所も特定することができる。ここで注意すべきは、デジタルカメラ５１０で生成されたJPEG画像は、５１０－５２０間での鍵（Kdc）による認証、５２０－５３０間での鍵（Kpc）による認証、５３０－５４０間での鍵（Kapp）による認証により（つまり複数の認証を経て）守られていることである。このように高度なセキュリティを保持することにより、デジタルコンテンツの証拠能力を飛躍的に高めることができる。なおドライバ５３０および電子透かしの埋め込みを行う登録アプリケーション５４０の動作するPCを、電子透かしを埋め込む装置として実施してもよいし、埋め込まれた電子透かしを抽出し、JPEG画像の改ざん場所を特定するアプリケーション５５０が動作するPCを、専用の電子透かし抽出装置として実施してもよい。また電子透かしおよびその抽出を同一のPCで行っても何ら構わない。

【０１５４】図４６に本発明で用いるデジタルカメラ５１０とＣＦ５２０のハードウェアブロック図を示す。始めにデジタルカメラ５１０、ＣＦ５２０、ドライバ５３０の間では特定の共通のコマンド（Ｒｅｑｕｅｓｔ Ｓｅｅｄ コマンド、ＳｅｎｄＳｅｅｄ コマンド）を定義しておく。一般の装置はこれらのコマンドに対して、エラーを返すかタイムアウトになる。Ｒｅｑｕｅｓｔ Ｓｅｅｄコマンドはクライアントにシードを送信するよう要求するコマンドであり、Ｓｅｎｄ Ｓｅｅｄコマンドはクライアントにこれからシードを送信することを知らせるコマンドである。認証はこれららのコマンドをデバイス間で相互に発信し、要求された数列が返ってくるかどうかで行われる。次にデジタルカメラ５１０とＣＦ５２０は共通の鍵Kdcを持っている。該鍵Kdcはデジタルカメラ５１０のＲＯＭ領域に記憶されている。またＣＦ５２０のＮＡＮＤ領域５２１（Ｒｅａｄ／Ｗｒｉｔｅ可能なメモリ領域）にＣＦ５２０の鍵Kcfにより暗号化されて記憶されている。ＣＦ５２０のＮＡＮＤ領域に記憶する理由は、特定のデジタルカメラで使用したＣＦを多のデジタルカメラで利用する場合があるからである。ＣＦ５２０内のKdcは初期化の段階でどのデジタルカメラと一緒に使用されるかの情報として該鍵Kdcを保持する。なお初期化のプロセスを行うことにより、鍵Kdcは変更が可能である。また鍵KcfはＣＦ５２０を特定するための鍵である。またＣＦ５２０の記憶領域にはＲＡＭ領域５２５、ＮＡＮＤ領域５２１があるが、ＲＡＭ領域は主に演算、データの受け渡しなど臨時的に使用され、ＮＡＮＤ領域は画像データや鍵情報の保存に主に使用される。ＣＰＵ５２２は乱数発生、暗号化（ＲＣ４）のための演算、比較などを主に行う。ＣＦ５２０のＮＡＮＤ領域５２１には鍵Kcfにより暗号化された鍵Kdcのほかに、生の画像データ（ＪＰＥＧ）、分割された画像データから得られる暗号化データ、鍵Kpc、デジタルカメラIDファイル、使用者IDファイル、撮影日、ＣＦ５２０のシリアル番号などが記憶される。ＮＡＮＤ領域５２１の暗号化された鍵、データはＲＡＭ領域５２５のデータと異なり、通常の方法で読み取ってもそのデータは解読不能である。また各鍵データベース５６０、５７０，５８０、５９０は、予め各デバイスに記憶されるべき鍵情報を有している。この鍵情報を使用して各デバイスは認証を行う。鍵データベース５６０には、デジカメ使用機器ＩＤと秘密鍵Kdcの組が保存されている。鍵データベース５７０には、使用者ＩＤと秘密鍵Kpcの組が保存されている。これらのデータベースはＣＦ５２０の初期化の時に使用される。ＣＦ５２０はデジタルカメラの内部にセットされる前に以下の手順で初期化される。

（１）使用者ＩＤをＣＦ５２０内のＲＡＭ領域５２５に保存する。

（２）鍵KpcをＣＦ５２０内のＮＡＮＤ領域５２１に保存する。

（３）使用機器ＩＤファイルをＣＦ５２０内のＮＡＮＤ領域５２５に保存する。

（４）鍵KdcをＣＦ５２０内のＮＡＮＤ領域５２１に保

存する。
ＣＦ５２０のＮＡＮＤ領域に保存されている鍵Kdc、Kpcは各デバイスとの認証に使用する数列作成に用いられる。このように初期化されたＣＦ５２０とデジタルカメラは次のようにして認証とデータの保存を行う。まずデジタルカメラ５１０の認証部５１３とＣＦ５２０の認証部５２３は共通の鍵Kdcを用いた認証を行う。認証成功に伴い、デジタルカメラ５１０は、ＣＣＤ等などのデバイスからなる画像取り込み部５１１にて画像信号を発生させ画像処理部５１２に送られ画像データとなる、この画像データがＣＦ５２０のＮＡＮＤ領域５２１に書き込まれる。ただしこのとき平行してその画像データは随時５１２バイトづつ、鍵KcfおよびＣＦ５２０のシリアル番号により暗号化されてＮＡＮＤ領域５２１に暗号データとして書き込まれる。好適にはＲＯＭ領域５２３をタンパープルーフにしておく。以降ＣＦ５２０内に画像を保存するという場合、ＮＡＮＤ領域５２１に画像データそのものが記憶され、さらにＮＡＮＤ領域５２１には分割画像データから得られる暗号化されたデータが保存されることを意味数する。
【０１５５】図３１にデータ鑑定方法のメイン・フローチャートを示す。ステップＳ１０００はJPEG画像生成を行うステップである。デジタルカメラ５１０でJPEG画像を生成し、Ｓ２０００の、５１０-５２０間認証に渡す。ステップＳ２０００は、５１０-５２０間認証を行うステップである。デジタルカメラ５１０とＣＦ５２０間で認証を取り合い、その結果とJPEG画像をＣＦに保存する。ステップＳ３０００は、５２０-５３０間認証を行うステップである。ＣＦ５２０とＣＦ用ドライバ５３０間で認証を取り合い、その結果をＳ４０００の５３０-５４０間認証に渡す。ステップＳ４０００は、５３０-５４０間認証を行う。ＣＦ用ドライバ５３０とJPEG画像登録・保存アプリケーション５４０間で認証を取り合い、その結果をＳ５０００の５４０－５５０間認証に渡す。ステップＳ５０００はID等埋め込みを行うステップである。Ｓ２０００の５１０－５２０間認証、Ｓ３０００の５２０-５３０間認証、Ｓ４０００の５３０-５４０間認証の結果を表示し、JPEG画像にID、改ざん有無検出用マークを埋め込む。ステップＳ６０００はID等抽出／検出を行うステップである。JPEG画像に埋め込まれたIDを抽出、改ざん有無検出用マークを検出し、その結果を表示する。また改ざんがあった場合は改ざん場所をJPEG画像とともに表示する。
【０１５６】次にステップＳ２０００の５１０-５２０間認証のフローチャートを図３２に示す。ステップＳ２１００は５１０－５２０間認証判定を行うステップである。５１０－５２０間の認証用鍵（Kdc）によりデジタルカメラ５１０とＣＦ５２０間の認証をした後、Ｓ１０００のJPEG画像生成により生成されたJPEG画像と認証結果を出力する。ステップＳ２２００はＣＦ５２０へのJPEG保存を行うステップである。Ｓ２１００の判定結果とJPEG画像をＣＦ５２０内JPEG画像保存用鍵（Kcf）を用いて、ＣＦ５２０内にJPEG画像を保存する。
【０１５７】次にステップＳ２１００の５１０-５２０間認証判定の詳細フローチャートを図３３に示す。まずＳ２１００でＣＦ５２０が乱数の数列(a)を生成する。そしてＣＦ５２０はこの生成した数列(a)をデジタルカメラ５１０へ送る。ステップＳ２１２０でデジタルカメラ５１０は受け取った数列(a)をデジタルカメラ５１０内部に持つ鍵Kdcを用いて暗号化する。そしてその暗号化の出力である数列（ｂ）を生成する。ここでＣＦ５２０はステップＳ２１３０で独自に乱数(a)からＣＦ内部に持つ鍵Kdcを入力としてＲＣ４の暗号化（演算は図４６のＣＦ５２０内のＣＰＵ５２２により行われる）を行い、その出力である数列（ｃ）を生成する。そしてステップＳ２１４０で、ＣＦ５２０は、デジタルカメラ５１０で計算された送られた数列（ｂ）と内部で作成した数列（ｃ）を比較する。その比較の結果、同じだった場合はデジタルカメラ５１０とＣＦ５２０が持つ鍵Kdcは共通のものであるから、デジタルカメラとＣＦの認証は成功、違っていた場合は、デジタルカメラとＣＦ５２０の認証は失敗としてＳ２１００の判定結果を得る。
【０１５８】次にステップＳ２２００のＣＦ５２０への保存の詳細フローチャートを図３４に示す。デジタルカメラ５１０とＣＦ５２０間の認証が成功した場合、次にデジタルカメラ５１０で生成された画像をＣＦ５２０内にKcfを用いて保存する。ステップＳ２２１０はJPEG画像分割を行うステップである。デジタルカメラ５１０で生成されたJPEG画像を５１２byteづつに分割する。ステップＳ２２２０は５１０-５２０間認証判定を行うステップである。Ｓ２１００の５１０－５２０間認証判定の出力結果である２１００判定結果から、デジタルカメラ５１０とＣＦ５２０間の認証が失敗している場合は、ＣＦ内のＮＡＮＤ領域に０の数列を書き込み、認証が成功している場合、ステップＳ２２３０でデジタルカメラ５１０で生成された画像をＣＦ５２０内の鍵Kcfを用いてＮＡＮＤ領域５２１に記憶する。この時鍵KcfはＣＦ５２０のＲＯＭ領域５２３に保存されている。Ｓ２２１０の出力結果である５１２byteのデータとＣＦ５２０のシリアル番号、ＣＦ５２０内に内蔵されている該鍵Kcfを用いてＲＣ４による計算を行い、その結果の数列をＣＦ５２０内のＮＡＮＤ領域５２１に書き込む。
【０１５９】次にステップＳ３０００の５２０－５３０間認証のフローチャートを図３５に示す。ステップＳ３１００は５２０－５３０間認証判定を行うステップである。５２０－５３０間の認証用鍵（Kpc）によりＣＦ５２０とＣＦドライバ５３０間の認証をした後、認証結果Ｓ３１００を出力する。
【０１６０】次にステップＳ３１００の５２０-５３０間認証判定の詳細フローチャートを図３６に示す。まず

鍵データベース５７０の中には予めＣＦ５２０の使用者ＩＤと鍵Kpcがペアとなって保存されている。またＣＦ５２０内には、使用者ＩＤ、鍵KpcがＮＡＮＤ領域５２１に保存されている。ステップＳ３１１０は５２０-５３０間認証用乱数生成を行うステップである。ＣＦドライバ５３０が認証のために使用する乱数（ａ）を生成する。ステップＳ３１２０はＣＦ５２０において認証用数列を生成するステップである。ＣＦ５２０内のＮＡＮＤ領域５２１にあらかじめ入っている鍵Kpcと、Ｓ３１１０の出力結果である乱数（ａ）を使って、ＲＣ４によって計算される数列（ｂ）を出力する。ステップＳ３１３０はＣＦドライバ５３０側での認証用数列生成を行うステップである。ＣＦドライバ５３０は鍵Kpcと、Ｓ３１１０の出力結果である乱数（ａ）を使って、ＲＣ４によって計算される数列（ｃ）を出力する。ステップＳ３１４０は５２０-５３０間認証用数列判定を行うステップである。ＣＦドライバ５３０がＳ３１２０の出力結果である数列（ｂ）とＳ３１３０の出力結果である数列（ｃ）を比較し、両者が同じ物であった場合「ＣＦとＣＦドライバ間の認証は成功」という結果を出力する。両者が違う物であった場合「ＣＦとＣＦドライバ間の認証は失敗」という結果を出力する。好適には、認証失敗の場合、これ以降の認証の処理を行わないで、アプリケーション５４０上でＣＦ５２０内の画像が表示される時、「コンパクトフラッシュドライバとコンパクトフラッシュ間の認証に失敗しているため、オリジナリティーが確認できない画像です」という警告メッセージを表示装置１００に表示する。

【０１６１】次にステップＳ４０００の５３０-５４０間認証のフローチャートを図３７に示す。ステップＳ４１００は５３０－５４０間認証判定を行うステップである。５３０－５４０間の認証用鍵（Kapp）によりＣＦドライバ５３０とJPEG画像登録・保存アプリケーション５４０間の認証をした後、認証結果Ｓ４１００を出力する。

【０１６２】次にステップＳ４１００の５３０-５４０間認証の詳細フローチャートを図４０に示す。このステップＳ４１１０ではまずアプリケーション５４０が認証のために使用する乱数（ａ）を生成する。ステップＳ４１２０はＣＦドライバ５３０が認証用数列（ｂ）を生成するステップである。ＣＦドライバ５３０は鍵Kappと、Ｓ４１１０の出力結果である乱数（ａ）を使って、ＲＣ４によって計算される数列（ｂ）を出力する。ステップＳ４１３０はアプリケーション５４０が認証用数列（ｃ）を生成するステップである。アプリケーション５４０は、アプリケーション５４０内にあらかじめ入っている鍵Kappと、Ｓ４１１０の出力結果である乱数（ａ）を使って、ＲＣ４によって計算される数列（ｃ）を出力する。ステップＳ４１４０は５３０－５４０間認証用数列判定を行うステップである。Ｓ４１２０の出力結果である数列（ｂ）とＳ４１３０の出力結果である数列（ｃ）を比較し、両者が同じ物であった場合「ＣＦドライバとアプリケーション間の認証は成功」という結果を出力する。両者が違う物であった場合「ＣＦドライバとアプリケーション間の認証は失敗」という結果を出力する。好適には、認証が失敗した場合、これ以降の認証の処理を行わないで、アプリケーション５４０上でＣＦ５２０内の画像が表示される時、「アプリケーションとコンパクトフラッシュ・ドライバ間認証に失敗しているため、オリジナリティーが確認できない画像です」という警告メッセージを表示装置１００に表示する。使用者によりデータベースに登録するために選ばれた画像が「オリジナリティーが確認できない画像」だった場合は、画像に電子透かしにより埋め込まれる情報の中に「登録する前にオリジナリティーが確認されなかった画像」（すなわち出所が確認されなかった画像）という情報を含ませる。

【０１６３】次にステップＳ５０００のID等埋め込みのフローチャートを図３８に示す。ステップＳ５１００はＣＦ５２０内のJPEG検査を行うステップである。ＣＦ５２０内に保存されてるJPEG画像に改ざんが行われたかどうかを検査する。ステップＳ５２００はID埋め込みを行うステップである。データ埋め込み／抽出用鍵（Kdh）を用いて、イメージID（ＩＤ情報）をJPEG画像に電子透かしにより埋め込む。

【０１６４】次にステップＳ５１００のＣＦ５２０内JPEG検査の詳細フローチャートを図３９に示す。ステップＳ５１１０はＣＦ５２０内JPEG画像分割を行うステップである。ＣＦ５２０内に保存されているJPEG画像を５１２byteづつに分割する。ステップＳ５１２０はデータ判定用数列生成を行うステップである。アプリケーション５４０はＳ５１１０の出力結果である５１２byteのデータとＣＦ５２０のＮＡＮＤ領域５２１に記憶されているシリアル番号、ＣＦ５２０内のＲＯＭ領域５２３に内蔵されている鍵Kcfを用いてＲＣ４を行い、その結果の数列(a)を出力する。ステップＳ５１３０はデータ判定用数列読取りを行うステップである。ＣＦ５２０内のＮＡＮＤ領域５２１に書かれている数列（b）を出力する。ステップＳ５１４０はデータ判定用数列比較を行うステップである。Ｓ５１２０の出力結果である数列（a）とＳ５１３０の出力結果である数列（b）を比較し、両者が同じ物であった場合「５１２byteのデータは改ざんがされていない」という結果を出力し、分割された次のデータへ処理を進める。両者が違う物であった場合「５１２byteのデータは改ざんがされているので、このJPEGデータは改ざんされている」という結果を判定結果Ｓ５１００として出力する。

【０１６５】次にステップＳ５２００のID埋め込みの詳細フローチャートを図４１に示す。ステップＳ５２１０はイメージID生成を行うステップである。JPEG画像に電

子透かしによって埋め込むデータ（イメージID）を生成する。イメージIDは判定結果Ｓ３１００、判定結果Ｓ４１００、判定結果Ｓ５１００による認証履歴情報、撮影日、撮影者（使用者ＩＤ）、登録日、撮影機器（デジタルカメラＩＤ）などから生成される数列である。ここでいう認証履歴情報とはデジタルカメラ５１０から、JPEG画像登録・保存アプリケーション５４０の間の認証はすべて成功しているか、あるいは失敗しているかという情報、ＣＦ５２０内JPEG画像の改ざんの有無をあらわす情報などを含む、いわゆる過去の認証の履歴を表わす情報である。後程この認証履歴情報を抽出することによりどの時点で認証ができなくなったか(どの過程で改竄された可能性があるか)が分る。ステップＳ５２２０はイメージID埋め込みを行うステップである。データ埋め込み／抽出用鍵（Kdh）を用いて、イメージIDをJPEG画像に電子透かしにより埋め込み電子透かしが施されたJPEG画像を出力する。

【０１６６】次にステップＳ６０００のID等抽出／検出の詳細フローチャートを図４２に示す。ステップＳ６１００はID抽出を行うステップである。データ埋め込み／抽出用鍵（Kdh）を用いて、イメージIDをJPEG画像から電子透かしにより抽出する。ステップＳ６２００は抽出検出結果解析表示を行うステップである。Ｓ６１００（ID抽出）で抽出したＩＤ、改ざんの有り無し、（改ざんがあった場合）改ざん場所をJPEG画像とともに表示する。

【０１６７】次にステップＳ６１００のID抽出のより詳細なフローチャートを図４３に示す。ステップＳ６１１０はイメージID抽出を行うステップである。JPEG画像から電子透かしによって埋め込まれたデータ（イメージID）をデータ埋め込み／抽出用鍵（Kdh）を用いて抽出する。ステップＳ６１２０はイメージID解析 改ざん有無判定を行うステップである。Ｓ６１１０の出力結果から認証履歴情報、撮影日、撮影者、登録日、撮影機器などを解析し、さらに画像中に改ざんされている場所があるかどうかを電子透かしを用いて検査する。その結果、改ざん場所が観測された場合は、Ｓ６１３０（改ざん場所特定）処理に移り、改ざん場所がなかった場合は、解析した結果（認証履歴情報、撮影日、撮影者、登録日、撮影機器など）をＳ６１００検出結果として出力する。ステップＳ６１３０は改ざん場所特定を行うステップである。Ｓ６１２０の結果が改ざんあり、と判定された場合、改ざん場所特定処理を行い、改ざん場所を二値画像化し、Ｓ６１２０の解析した結果（認証履歴情報、撮影日、撮影者、登録日、撮影機器など）とともにＳ６１００検出結果として出力する。

【０１６８】［保険業務］図４４に、本発明のデータ鑑定装置を用いたクレームサービス、損害査定業務の概要を示す。本発明は、保険の掛けられた対象に損害を生じ、契約者から保険会社に損害保険の支払い請求があった場合に、保険会社が調査に基づいて損害額を査定し保険金の支払いを行う、損害査定業務などにそのまま適用できる。本発明のデータ鑑定装置を用いることにより損害対象の証拠デジタル写真が改ざんやすり替え等から守られ、損害査定業務を安全かつ効率的に行う事ができる。なお同様に、損害保険業務に関わらず、証拠書類として対象物や現場の写真を用いる土木・建築業務、官公庁の不動産管理、環境開発・保全、災害対策などの広汎な業務に適用できる。図４４の損害査定業務の概要を自動車保険のケースに適用して説明する。 保険を契約している顧客またはその代理店６４０から事故の報告を受けた保険会社６６０は、ただちにその事故を担当する保険会社支社６５０に通報する。保険会社の支社マネージャは、査定員６３０を指名し、損害調査の指示をする。査定員６３０は損害車両が保管されている修理工場などに赴き車両を調査し、デジタルカメラを用いて損害の証拠のため写真撮影を行い、損害額の査定を行う。また査定員６３０はPCを用いてこの事故案件についての詳細／証拠写真ファイルが添付された査定書を作成する。そして査定員６３０は査定書を、支店マネージャの承認を受けるために提出／事故案件データベース６００に登録する。支店マネージャは査定員の提出した事故案件を鑑定／承認し、保険金の支払いが行われる。

【０１６９】［保険業務プロセス］次に、本発明の方法が組み込まれた損害査定業務プロセスの流れを図４５に示す。まず査定員６３０がデジタルカメラ５１０で撮った写真が、デジタルカメラ内でJPEG画像として生成される。次に生成されたJPEG画像はデジタルカメラ５１０内に入れられているコンパクトフラッシュ５２０に相互認証の後、各々保存される。査定員６３０は、ＣＦ５２０内のJPEG画像を損害査定業務アプリケーション内に登録するために、ＣＦ５２０内に保存されているすべてのJPEGを一覧表示から、登録写真として選択する。損害査定業務アプリケーション５４０はJPEG写真の一覧表示時、ＣＦ５２０とＣＦ用ドライバ５３０の相互認証、ＣＦ用ドライバ５３０と損害査定業務アプリケーション５４０の相互認証を行い、かつ、デジタルカメラ５１０とＣＦ５２０の相互認証の結果、ＣＦ５２０内に保存されているすべてのJPEGに対して、入力の正当性を検査し、その結果を表示する。査定員６３０は、その結果を参照しつつ、事故案件として登録すべき写真を選択する。これにより、信頼のおけるJPEG画像かそうでないか確認できる。認証の結果が無いかもしくは認証に失敗した情報を有する写真は、別に撮影された写真画像がPCで改ざんされた後、このＣＦ５２０に書き込まれた可能性を否定できないので、以下の業務で使用しないと決めれば、この不正行為を未然に防ぐことができる。次に査定員６３０によって選択されたJPEG写真が事故案件データベース６００に保存される。この時、保存されるJPEG写真に、電子透かしにより改ざん有無検出用マークと、撮影日・登

録日・撮影者・認証履歴情報・使用機器等により作られるイメージIDが埋め込まれる。そして損害査定業務アプリケーション５４０内に登録されているJPEG写真を保険会社マネージャが鑑定する。この時、事故案件データベース６００に登録されているJPEG写真は、電子透かしによりに改ざん有無の検出と、イメージIDの抽出が行われ、その結果が損害査定業務アプリケーション上に表示される。また、JPEG写真がアプリケーション登録後に改ざんされた場合、その改ざん場所も表示する。なお、改ざん有無の検出を行うＰＣは、埋め込みと同一のＰＣでも構わないし、通信で結ばれた遠隔ＰＣ６１０でも構わない。

【０１７０】本発明は、本人証明を行うシステムに容易に応用できる。図４７に本発明をスマートカードに応用した例を示す。スマートカード７００には表面に、その所有者の名前、ＩＤ番号などが記載されている。好適には本人の写真イメージなどが印刷されている。本スマートカードの特徴的な所は、このような本人を証明するデータをスマートカード内のメモリ領域に電子透かしと埋め込まれている点にある。この電子透かしには、本発明の改変個所特定を行う改変検出用データを有しているので、改ざん及び改ざん個所の特定が行える点にある。本人証明を行う証明データ検出方法は、該スマートカート７００をスマートカード・リーダ７１０に読み込ませ、改変検出用データが埋め込まれた所有者の証明データをスマートカードから読み取り、改変検出用データの抽出結果に基づき、前記証明データ改変の有無の判断を行い、改変がなされたと判断した場合に改変個所の特定を行う。なお、本人証明データとは、その人物の書誌的なデータのほか生物学的特徴である、指紋、声紋、虹彩、網膜などの電子化されたデータをスマートカード７００に本発明の改変検出用データを有する電子透かしで記憶しておき、これをスマートカード・リーダ７１０で読み取り、改変を検知するようにする。改変があった場合にはどこに改変があったかを指摘する。好適には、改ざんがないと判定した後、スマートカード・リーダで読み取った情報を、窓口にきた人物から得られる情報と比較することにより、最終的な本人証明を終了する。

【０１７１】［コンテンツデータ鑑定装置の変形例］以下、本発明のデータ鑑定装置のその他の変形例を示す。図２７に図２６をよりシンプル（ＰＣに付属品としてデジタルカメラ５１０が接続される）にしたデータ鑑定装置を図示する。登録アプリケーション５４０でJPEG画像は鍵（Kdh）によるJPEGのID埋め込み（電子透かし）を施された後、ハードディスク上に保存される。表示アプリケーション５５０は登録アプリケーション５４０で埋め込まれたIDをJPEG画像から抽出し、また改ざんが有るかどうかを検査し、その結果を表示する。もし改ざんが合った場合は、改ざん場所も検出し表示する。

【０１７２】図２８に、図２６におけるデジタルカメラ５１０上で電子透かしを施すケースを示す。デジタルカメラ５１０で生成されたJPEG画像は、鍵（Kdh）によるJPEGのID埋め込み（電子透かし）を施される。メディア５２０に保存されたJPEG画像は、ドライバ５３０を経て、PC上の登録アプリケーション５４０によりハードディスク上に保存される。表示アプリケーション５５０はデジタルカメラ５１０で埋め込まれたIDをJPEG画像から抽出し、また改ざんの有無を検査し、その結果を表示する。もし改ざんが合った場合は、改ざん場所も検出し表示する。上記の認証、電子透かしは鍵によって守られているが、これらをタンパープルーフによって守ることにより、機密性がさらに高まる。

【０１７３】図２９に、図２６にのデジタルカメラ５１０からＰＣへケーブルにより直接接続したケースを示す。デジタルカメラ５１０で生成されたJPEG画像は、５１０－５３０間での鍵（Kpc）による認証と、５３０－５４０間での鍵（Kapp）による認証によって守られる。登録アプリケーション５４０でJPEG画像は、鍵（Kdh）によるJPEGのID埋め込み（電子透かし）を施された後、ハードディスク上に保存される。表示アプリケーション５５０は登録アプリケーション５４０で埋め込まれたIDをJPEG画像から抽出し、また改ざんの有無を検査し、その結果を表示する。もし改ざんが合った場合は、改ざん場所も検出し表示する。上記の認証、電子透かしは鍵によって守られているが、これらをタンパープルーフによって守ることにより、機密性がさらに高まる。

【０１７４】図３０に、より柔軟性のあるデータ鑑定装置を示す。デジタルカメラ５１０で生成されたJPEG画像は、５１０－５２０間での鍵（Kdc）による認証と、５２０－５３０間での鍵（Kpc）による認証と、５３０－５４０間での鍵（Kapp）による認証とによって守られる。登録アプリケーション５４０でJPEG画像は、鍵（Kdh）によるJPEGのID埋め込み（電子透かし）、鍵（Kalt）による改ざん有無検出用マークの埋め込み（電子透かし）を施された後、ハードディスク上に保存される。表示アプリケーション５５０は登録アプリケーション５４０で埋め込まれたIDをJPEG画像から抽出し、また改ざんが有るかどうかを検査し、その結果を表示する。もし、改ざんがあった場合は、改ざん場所も検出し表示する。ここで注目すべきは、JPEG画像データそのものから得られるハッシュ値により計算された鍵（Kalt）のJPEGへのID埋め込みである。埋め込まれた鍵（Kalt）の値と、JPEG画像データから計算されるハッシュ値を比較することで、画像データに改ざんがあるかどうかの判断は瞬時に計算される。この鍵（Kalt）により、改変の有無の判断のみを高速に行うことで改ざんがない場合の処理が高速化される。ただし改ざんがある場合には他のケースと同様に鍵（Kdh）により改ざん場所の特定が行われる。上記の認証、電子透かしは鍵によって守られているが、これらをタンパープルーフによって守ることによ

り、さらに機密性が高まる。

【０１７５】

【発明の効果】以上説明したように、本発明にかかるデータ鑑定装置およびその方法によれば、コンテンツデータの作成から改変判定までの間に関わる複数の装置間で、適切な認証を行うことにより、単にコンテンツデータの改変および改変個所の特定が行えるだけでなく、そのコンテンツデータに対する信頼性を非常に高くすることが可能になる。すなわち、デジタルカメラやデジタル録音装置などのデジタルデバイスを用いて作成された画像データ、音声データを証拠物件として扱えるようにするための、高度なセキュリティ保持のしくみが提供される。

【図面の簡単な説明】

【図１】本発明にかかる改変判定方法を実現する画像改変判定装置の構成を示す図である。

【図２】図１に示した画像改変判定装置が実行し、本発明にかかる改変判定方法を実現する埋込・判定プログラムの構成を示す図である。

【図３】図２に示した埋込部３０の構成を示す図である。

【図４】図３に示したデータ埋込部３２の構成を示す図である。

【図５】ディジタルカメラ（図１）が撮影した非圧縮画像データを例示する図である。

【図６】（Ａ）は、図５に例示した非圧縮画像データの一部を示す図であり、（Ｂ）は、（Ａ）に例示した非圧縮画像データ（部分）に含まれるＤＣＴブロック（マクロブロック）を示す図であり、（Ｃ）は、（Ｂ）に示したＤＣＴブロックそれぞれに含まれる８画素×８画素構成の画素を示す図である。

【図７】（Ａ）は、ディジタルカメラから入力される圧縮画像データを復号部がハフマン復号して得られる輝度信号ＹのＤＣＴ係数を示す図であり、（Ｂ）は、（Ａ）に示した輝度信号ＹのＤＣＴ係数の内、それぞれ隣り合う２組を対応付ける方法を示す図であり、（Ｃ）は、（Ｂ）に示した方法により対応付けられたＤＣＴ係数のペアを示す図である。

【図８】図２，３に示した埋込部が１つのペア（図７（Ａ），（Ｂ））に含まれるＤＣＴブロック（ブロック１，２）それぞれから選択した相互に対応するＤＣＴ係数を例示する図である。

【図９】（Ａ），（Ｂ）は、図８に例示したように選択されたブロック１，２それぞれのＤＣＴ係数を、埋め込みデータのビット（値１）を埋め込むために、ＤＣＴ係数の数値を変更する必要がある場合について例示する図である。

【図１０】図８に例示したように選択されたブロック１，２それぞれのＤＣＴ係数を、埋め込みデータのビット（値１）を埋め込むために、ＤＣＴ係数の数値を変更する必要がない場合について例示する図である。

【図１１】埋込部（図２，３）が、ＤＣＴブロックに対して埋め込みデータを埋め込むために用いられる埋め込みテーブルを例示する図表である。

【図１２】図４に示した係数操作部が、ＤＣＴブロックのペアに埋め込みデータを埋め込む処理（Ｓ１０）を示す図である。

【図１３】図２に示した抽出部の構成を示す図である。

【図１４】図１３に示した埋め込みデータ抽出部の構成を示す図である。

【図１５】（Ａ）は、埋込部（図２，３）が埋め込みデータを埋め込んだＪＰＥＧデータを伸長した画像を例示する図であり、（Ｂ）は、（Ａ）に示した画像に加えられた改変を例示する図であり、（Ｃ）は、改変後の画像を例示する図である。

【図１６】改変が加えられた部分を示す２値画像を、元の画像と合成して示す画像を例示する図である。

【図１７】クラスタリング処理により、改変が加えられた範囲を示す画像を、元の画像と合成して示す画像を例示する図である。

【図１８】埋込部（図２，３）が生成したＪＰＥＧデータに、改変・誤りが加えられていない場合に、抽出部が改変等がなされていないＪＰＥＧデータに含まれる各ペアから抽出するビットの値を示す図である。

【図１９】埋込部（図２，３）が生成したＪＰＥＧデータに、改変・誤りが加えられた場合に、抽出部が改変等がなされたＪＰＥＧデータに含まれる各ペアから抽出するビットの値を例示する図である。

【図２０】抽出部（図１３，１４）が、図１５に例示したように改変が加えられたＪＰＥＧデータから、図１９に例示したように改変等が加えられたペアを判定し、改変が加えられたペアの画像内における位置を示す２値画像を例示する図である。

【図２１】（Ａ）～（Ｄ）は、抽出部（図１３，１４）が、図１５に例示したように改変が加えられたＪＰＥＧデータから、図１９に例示したように改変等が加えられたペアを判定し、改変が加えられたペアが画像内において、いずれの範囲に存在するかを示すクラスタリング画像を例示する図である。

【図２２】図１４に示したデータ抽出部が、各ペアに埋め込まれた埋め込みデータのビットを抽出する処理を示すフローチャートである。

【図２３】図１に示した画像改変判定装置による埋め込みデータの埋め込み処理（Ｓ２０）を示すフローチャートである。

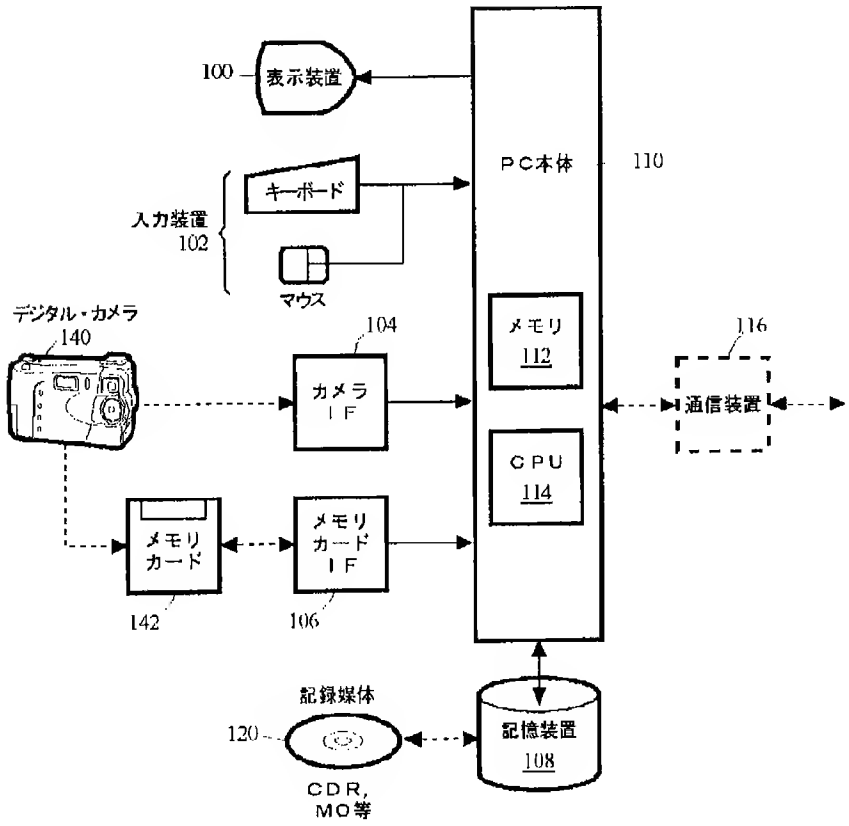
【図２４】図１に示した画像改変判定装置による埋め込みデータの抽出処理（Ｓ２２）を示すフローチャートである。

【図２５】それぞれ画像ＤＢを有する複数の画像改変判定装置を接続した改変判定システムの構成を示す図であ

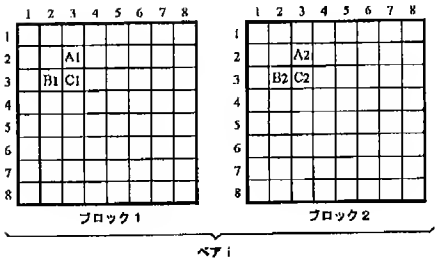
る。
【図２６】データ鑑定装置のブロック図である。
【図２７】ＰＣに付属品としてデジタルカメラ５１０が接続されるデータ鑑定装置である。
【図２８】デジタルカメラ５１０上で電子透かしを施すケースを示す図である。
【図２９】デジタルカメラ５１０からＰＣへケーブルにより直接接続したケースを示す図である。
【図３０】より柔軟性のあるデータ鑑定装置を示す図である。
【図３１】データ鑑定方法のメイン・フローチャートである。
【図３２】ステップＳ２０００の５１０-５２０間認証のフローチャートである。
【図３３】ステップＳ２１００の５１０-５２０間認証判定の詳細フローチャートである。
【図３４】ステップＳ２２００のＣＦ５２０への保存の詳細フローチャートである。
【図３５】ステップＳ３０００の５２０－５３０間認証のフローチャートである。
【図３６】ステップＳ３１００の５２０-５３０間認証判定の詳細フローチャートである。
【図３７】ステップＳ４０００の５３０-５４０間認証のフローチャートである。
【図３８】ステップＳ５０００のID等埋め込みのフローチャートである。
【図３９】ステップＳ５１００のＣＦ５２０内JPEG検査の詳細フローチャートである。
【図４０】ステップＳ４１００の５３０-５４０間認証の詳細フローチャートである。
【図４１】ステップＳ５２００のID埋め込みの詳細フローチャートである。
【図４２】ステップＳ６０００のID等抽出／検出のフローチャートである。
【図４３】ステップＳ６１００のID抽出のより詳細なフローチャートである。
【図４４】本発明のデータ鑑定装置を用いたクレームサービス、損害査定業務の概要を示す図である。
【図４５】本発明の方法が組み込まれた損害査定業務プロセスの流れを示す図である。
【図４６】本発明のデジタルカメラ５１０およびＣＦ５２０のハードウェアブロック図である。
【図４７】本発明のスマートカードおよびスマートカード・リーダの概観図である。
【符号の説明】
１，１－１～１－ｎ・・・画像改変判定装置
１００・・・表示装置
１０２・・・入力装置
１０４・・・カメラＩＦ
１０６・・・メモリカードＩＦ
１０８・・・記憶装置
１１０・・・ＰＣ本体
１１２・・・メモリ
１１４・・・ＣＰＵ
１１６・・・通信装置
１２０・・・記録媒体
１４０・・・ディジタルカメラ
１４２・・・メモリカード
２・・・埋込・判定プログラム
３，３－１～３－ｎ・・・埋込・抽出部
２０・・・埋込データ生成部
２２，２２－１・・・鍵情報ＤＢ
２４，２４－１～２４－ｎ・・・画像ＤＢ
２６・・・制御部
３０・・・埋込部
３００・・・復号部
３２・・・データ埋込部
３２０・・・画像分割部
３２２・・・乱数発生部
３２４・・・位置決め部
３２６・・・スクランブル部
３２８・・・係数操作部
３０４・・・符号化部
４０・・・抽出部
４００・・・復号部
４０２・・・画像分割部
４０４・・・符号化部
４０６・・・画像合成部
４２・・・埋込データ抽出部
４２０・・・乱数発生部
４２２・・・位置決め部
４２４・・・抽出順序生成部
４２６・・・対応付部
４２８・・・データ抽出部
４４・・・改変検出部
４６・・・クラスタリング部
５０・・・ＯＳ
５１０・・・デジタルカメラ
５１１・・・画像取り込み部
５１２・・・画像処理部
５１３・・・デジタルカメラ認証部
５２０・・・コンパクトフラッシュ（ＣＦ）
５２１・・・ＮＡＮＤ領域
５２２・・・ＣＦのＣＰＵ
５２３・・・ＲＯＭ領域
５２４・・・ＣＦ認証部
５２５・・・ＲＡＭ領域
５３０・・・コンパクトフラッシュ（５２０）用ドライバ・プログラム
５４０・・・JPEG画像登録・保存アプリケーション

５５０・・・JPEG画像表示・埋め込みデータ検出/抽出・改ざん場所検出アプリケーション
５６０・・・Kdc（５１０－５２０間の認証用鍵）のあるデーターベース
５７０・・・Kpc（５２０－５３０間の認証用鍵）のあるデーターベース
５８０・・・Kapp（５３０－５４０間の認証用鍵）のあるデーターベース
５９０・・・Kdh（データ埋め込み／抽出用鍵）のあるデーターベース
６００・・・事故案件データベース
６１０・・・埋め込みデータ検出/抽出・改ざん場所検出用ＰＣ
６３０・・・査定員
６４０・・・顧客／代理店
６５０・・・保険会社（支社）
６６０・・・保険会社（別の支社）
７００・・・スマートカード
７１０・・・スマートカード・リーダ

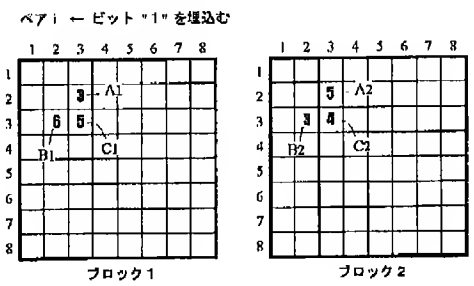
【図１】



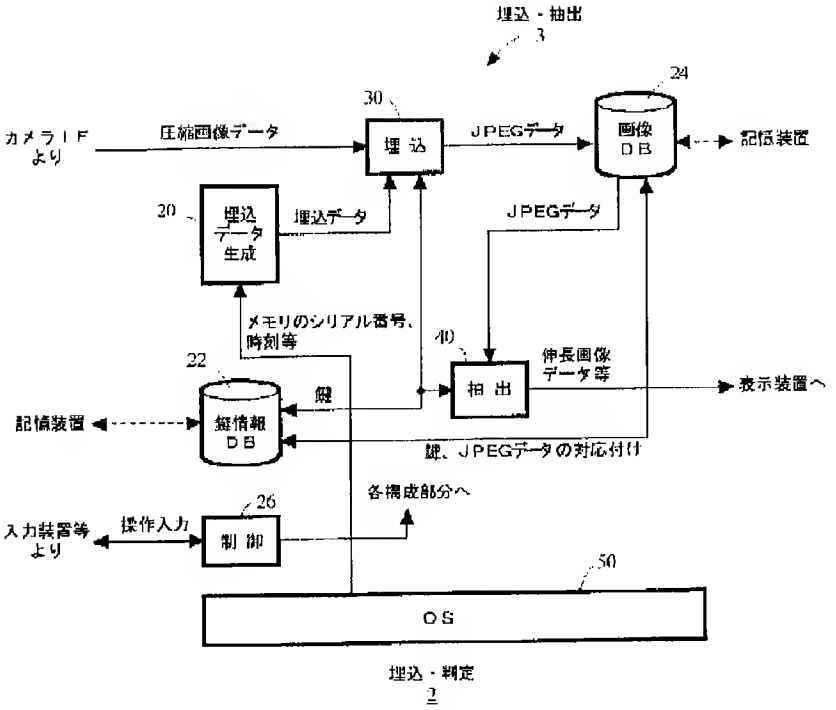
【図８】



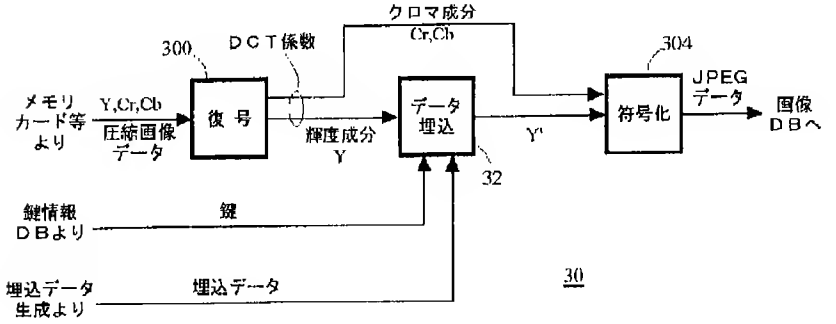
【図１０】



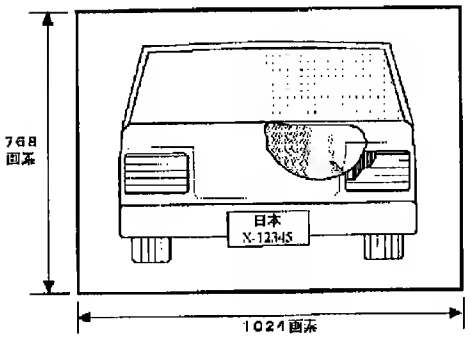
【図2】


埋込・抽出
3
24
30
カメラＩＦより
圧縮画像データ
埋込
JPEGデータ
画像DB
記憶装置
20
埋込データ生成
埋込データ
JPEGデータ
メモリのシリアル番号、時刻等
40
22
伸長画像データ等
抽出
表示装置へ
記憶装置
鍵情報DB
鍵
鍵、JPEGデータの対応付け
各構成部分へ
26
入力装置等より
操作入力
制御
50
OS
埋込・判定
2

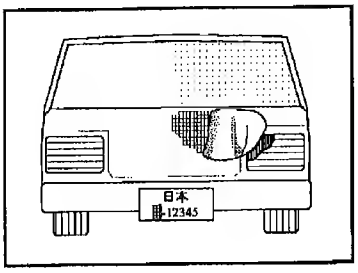
【図3】


クロマ成分
Cr,Cb
300
DCT係数
304
メモリカード等より
Y,Cr,Cb
圧縮画像データ
復号
輝度成分
Y
データ埋込
Y'
符号化
JPEGデータ
画像DBへ
32
鍵情報DBより
鍵
埋込データ生成より
埋込データ
30

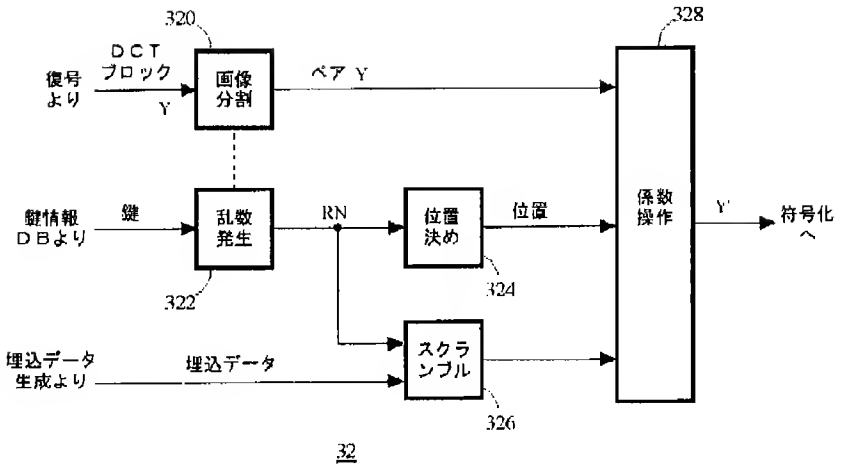
【図5】


768画素
日本
X-12345
1024画素

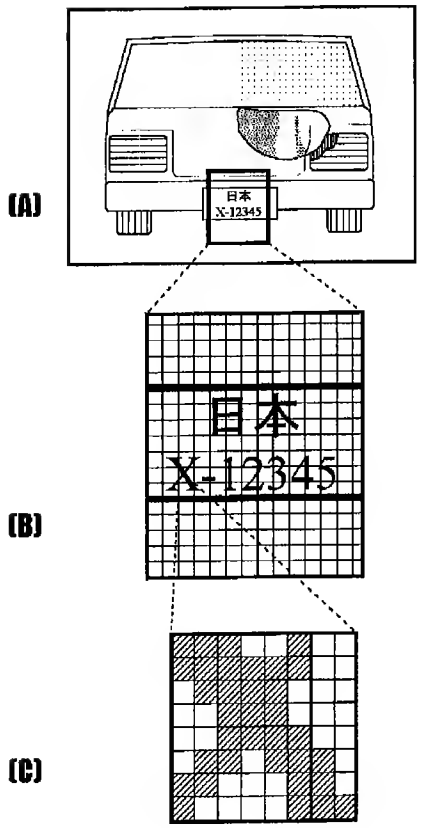
【図16】


日本
12345

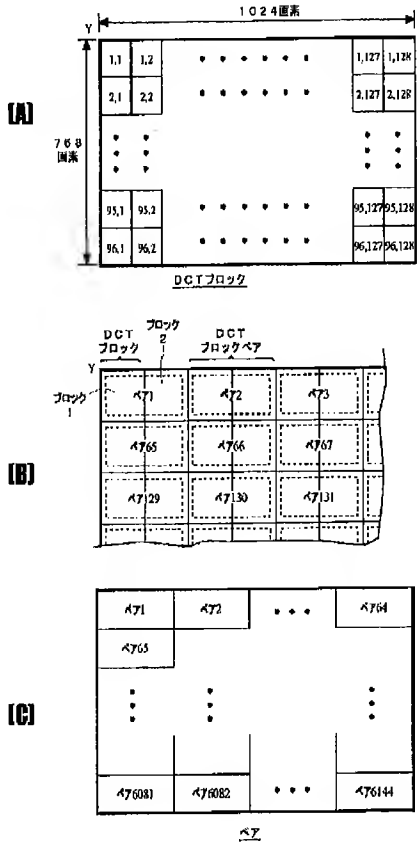
【図4】


320
DCT
ブロック
復号
より
Y
画像
分割
ペア Y
328
鍵情報
DBより
鍵
乱数
発生
RN
位置
決め
位置
係数
操作
Y'
符号化
へ
322
324
埋込データ
生成より
埋込データ
スクラ
ンブル
326
32

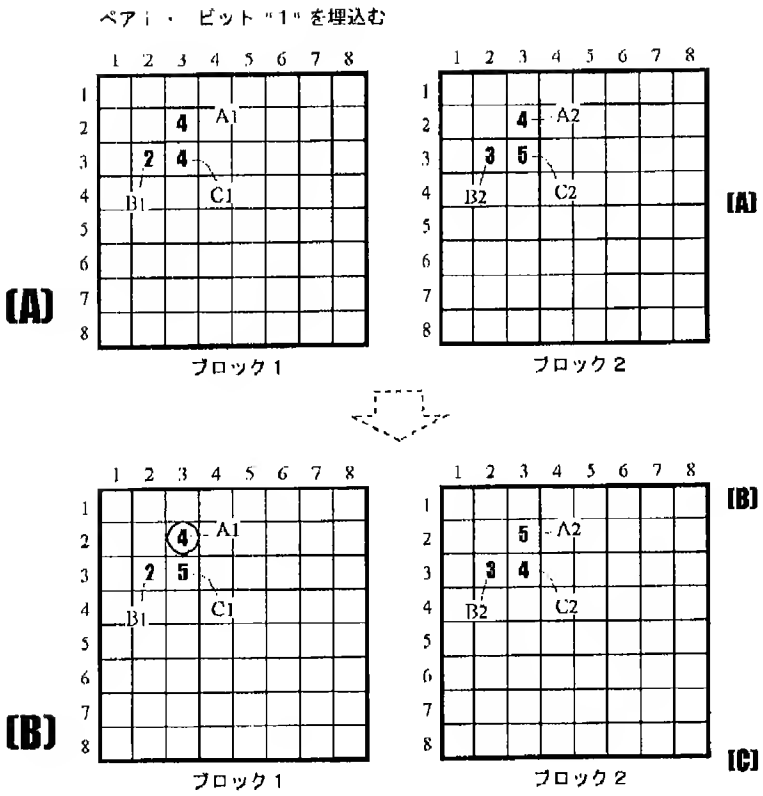
【図6】


(A)
日本
X-12345
(B)
日本
X-12345
(C)

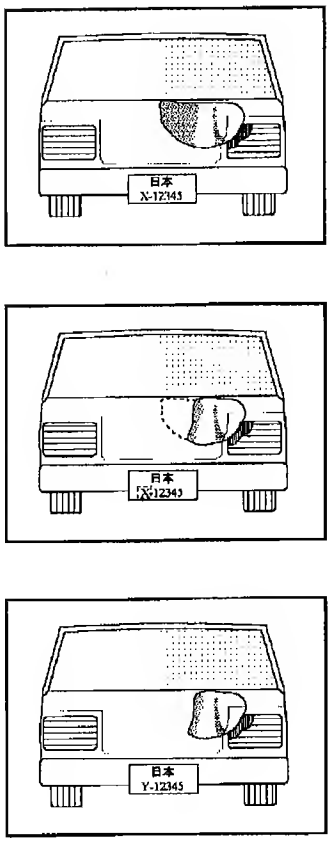
【図7】


(A)
1024画素
Y
768画素
1,1
1,2
1,127
1,128
2,1
2,2
2,127
2,128
96,1
96,2
96,127
96,128
DCTブロック
(B)
DCT
ブロック
ブロック
2
DCT
ブロックペア
ブロック
1
A71
A72
A73
A765
A766
A767
A7129
A7130
A7131
(C)
A71
A72
A764
A765
A76081
A76082
A76144
ペア

【図９】



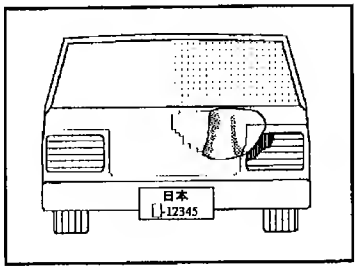
【図１５】



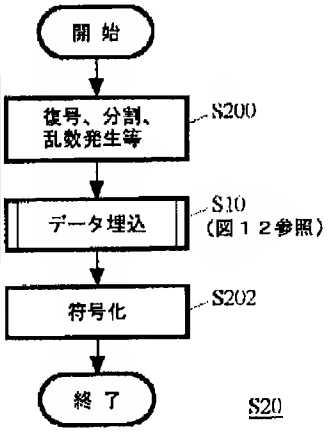
【図１１】

DCTブロックペア番号	ブロック１係数			ブロック２係数			埋込データビット番号	埋込データ割当て
	A1	B1	C1	A2	B2	C2	(1〜96)	
1	1	5	2	5	6	3	31	1
2	5	8	9	2	5	5	21	0
3	2	10	9	5	1	2	18	1
4	1	11	5	5	3	20	65	0
5	10	2	25	1	3	24	7	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
160	5	30	11	6	9	10	7	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
6144	51	20	11	3	19	15	34	1

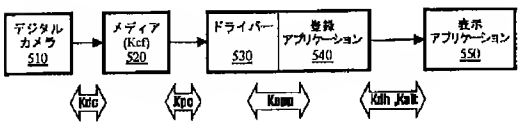
【図１７】



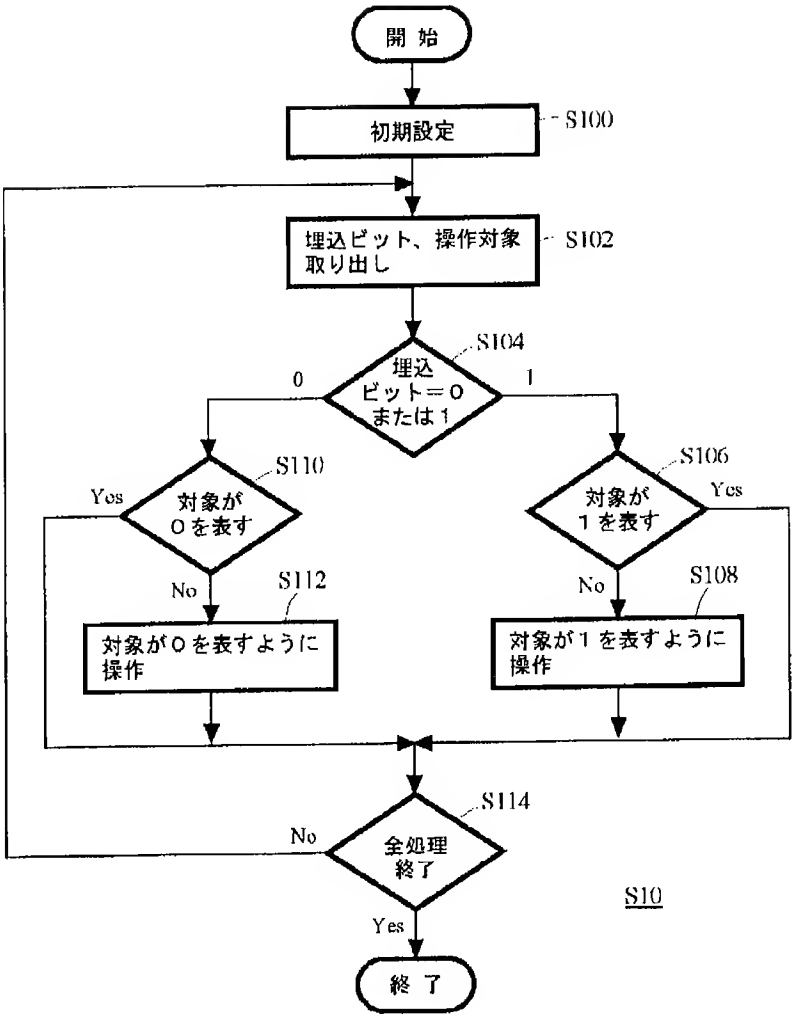
【図２３】



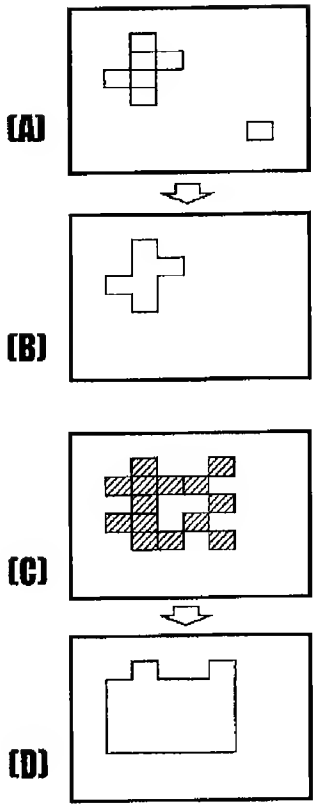
【図３０】



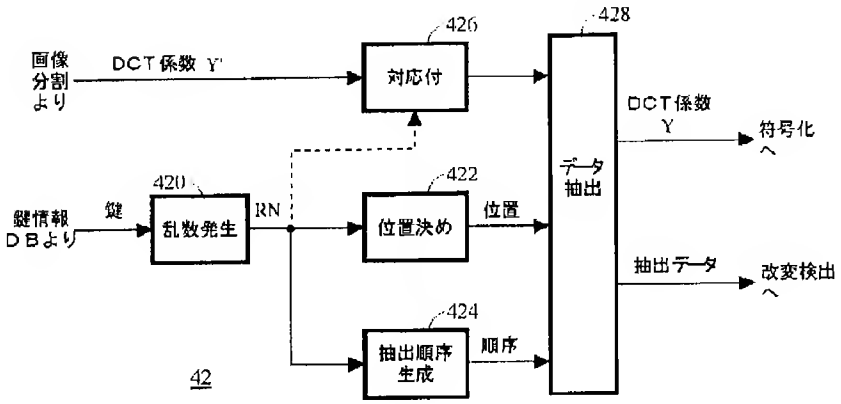
【図12】


開始
初期設定
S100
埋込ビット、操作対象取り出し
S102
S104
埋込ビット＝0または1
0
1
S110
対象が0を表す
Yes
No
S112
対象が0を表すように操作
S106
対象が1を表す
Yes
No
S108
対象が1を表すように操作
S114
全処理終了
No
Yes
終了
S10

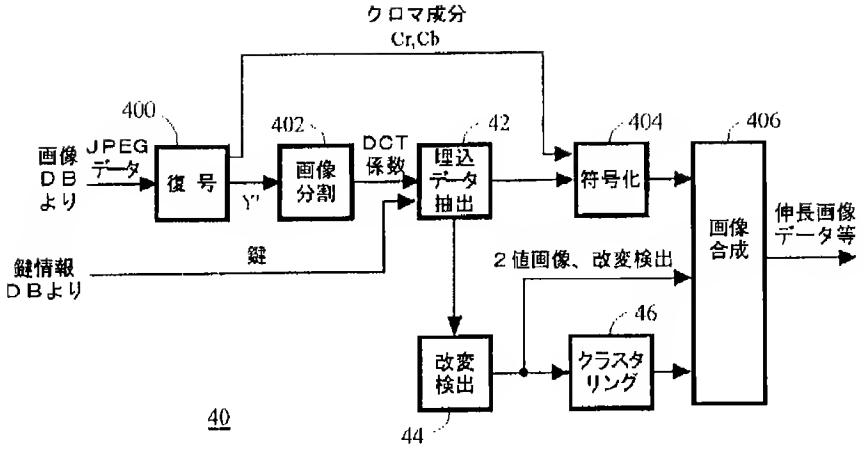
【図21】


(A)
(B)
(C)
(D)

【図14】


画像分割より
DCT係数 Y'
426
対応付
428
データ抽出
DCT係数 Y
符号化へ
鍵情報DBより
鍵
420
乱数発生
RN
422
位置決め
位置
抽出データ
改変検出へ
424
抽出順序生成
順序
42

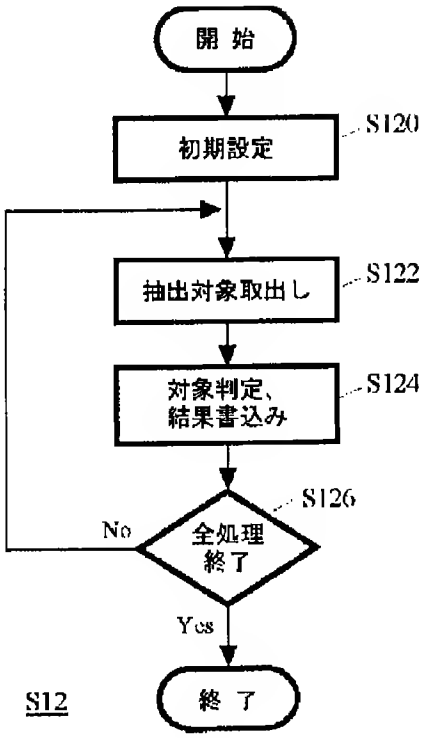
【図13】



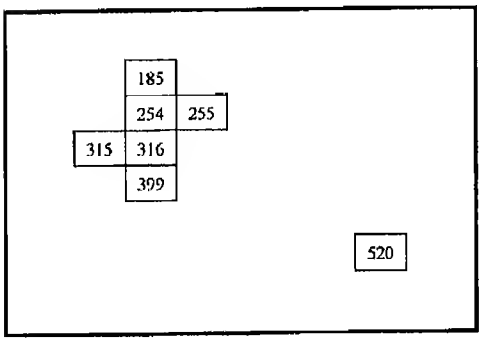
【図18】

	1	2	3	4	5		96	
ペア 1～96	ペア11 1	ペア5 0	ペア31 1	ペア9 1	0	- - - - - - - - - -	1	64回繰り返し
ペア 97～192	ペア99 1	ペア126 0	ペア150 1	ペア153 1	0	- - - - - - - - - -	1	
ペア 193～288	1	0	1	1	0	- - - - - - - - - -	1	
ペア 289～384	1	0	1	1	0	- - - - - - - - - -	1	
⋮	⋮	⋮	⋮	⋮	⋮		⋮	
ペア 6049～6144	1	0	1	1	0	- - - - - - - - - -	1	
抽出結果	1	0	1	1	0	- - - - - - - - - -	1	

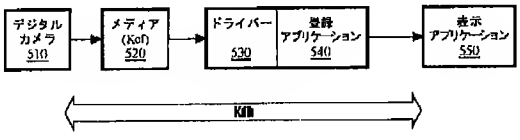
【図22】



【図20】



【図28】



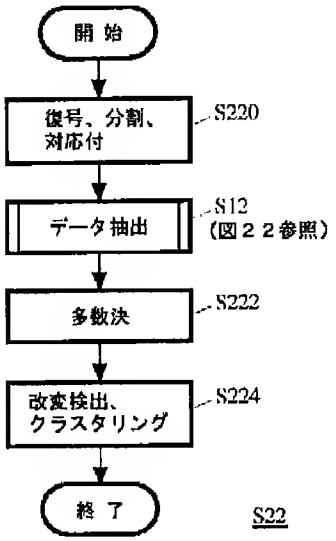
【図19】

検出された埋込データのビット番号

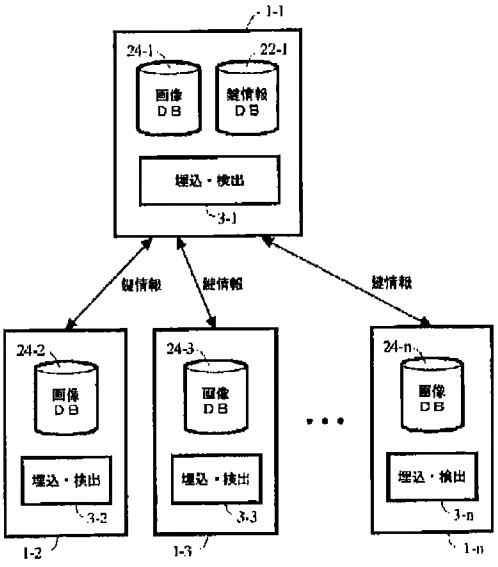
	1	2	3	4	5		96
ペア 1～96	ペア11 1	ペア5 0	ペア31 1	ペア9 1	0	- - - - - - - - - -	1
ペア 97～192	ペア99 1	ペア126 0	ペア150 1	ペア153 1	0	- - - - - - - - - -	ペア188 0
ペア 193～288	1	0	1	ペア255 0	0	- - - - - - - - - -	ペア254 0
ペア 289～384	1	ペア315 1	1	1	ペア316 1	- - - - - - - - - -	1
ペア 385～480	ペア399 0	0	1	1	0	- - - - - - - - - -	1
ペア 481～576	1	0	1	1	ペア520 1	- - - - - - - - - -	1
⋮	⋮	⋮	⋮	⋮	⋮		⋮
抽出結果	1	0	1	1	0	- - - - - - - - - -	1

不整合

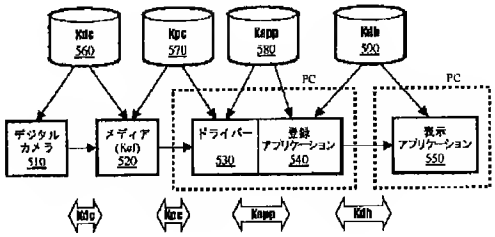
【図24】



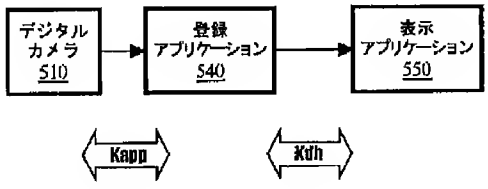
【図25】



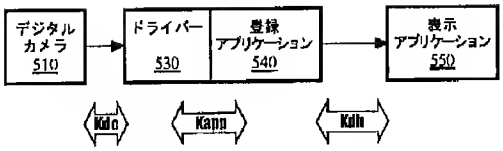
【図26】



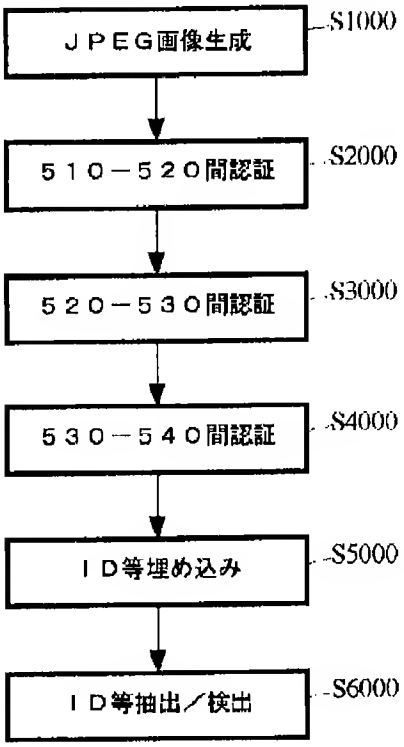
【図27】



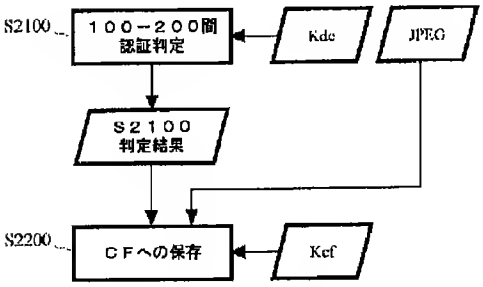
【図29】



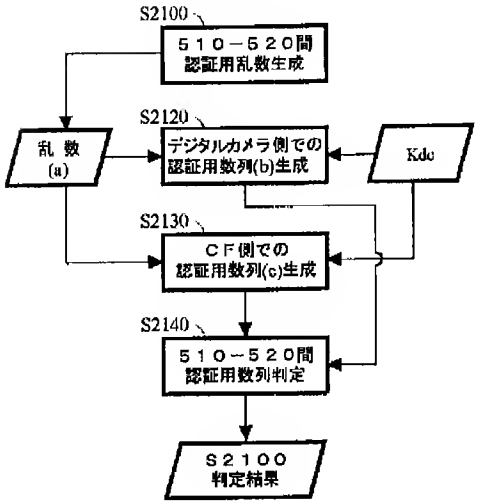
【図31】



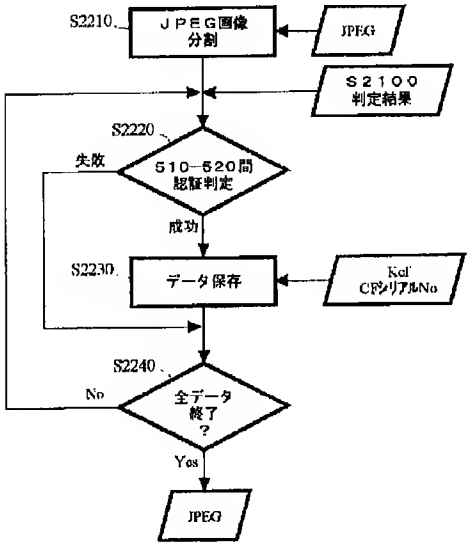
【図32】



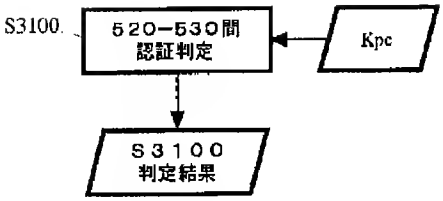
【図33】



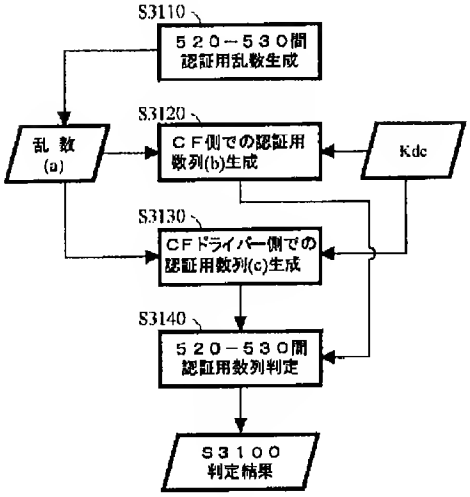
【図34】



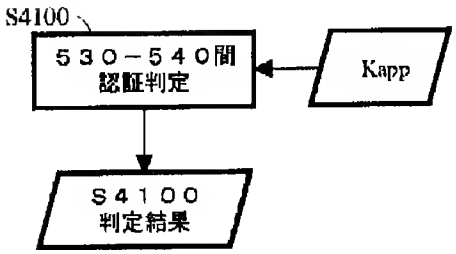
【図35】



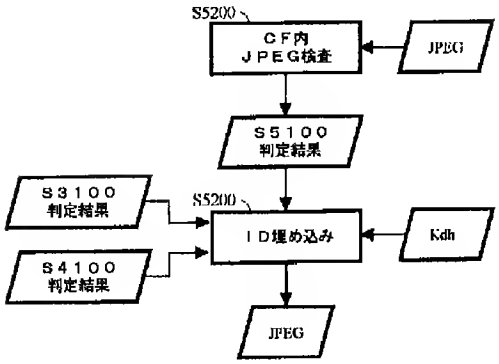
【図36】



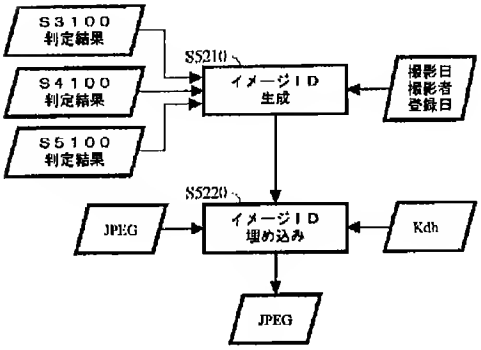
【図37】



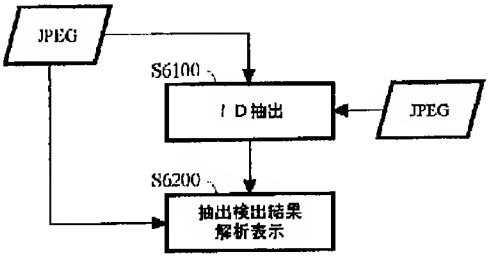
【図38】



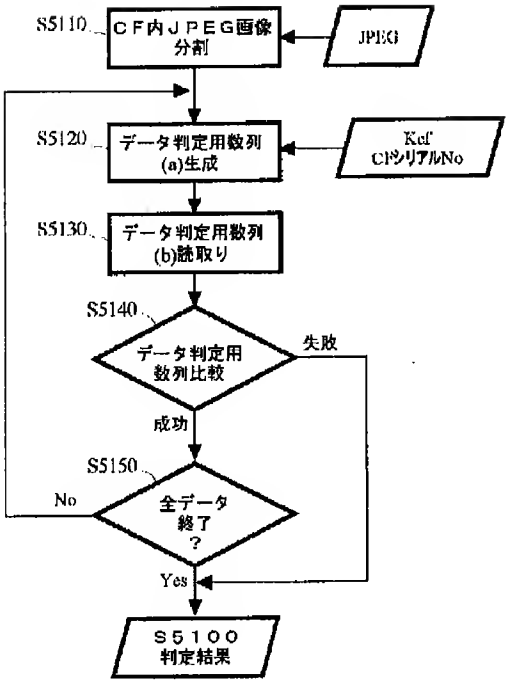
【図41】



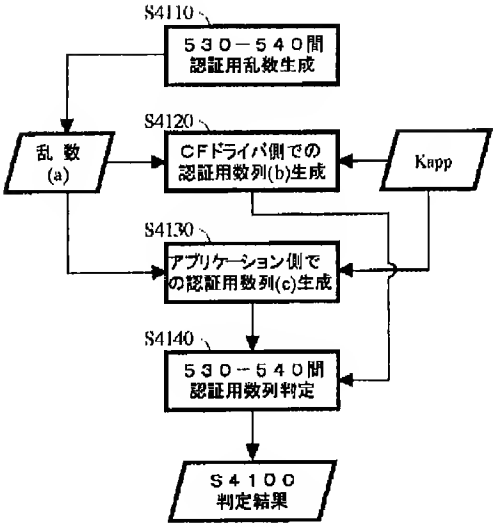
【図42】



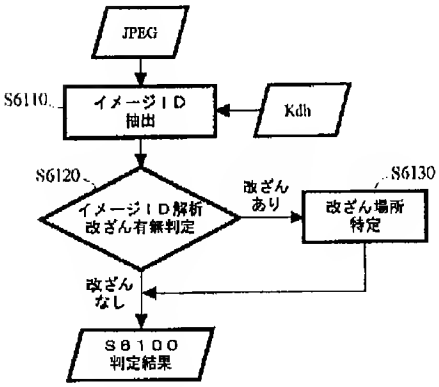
【図３９】



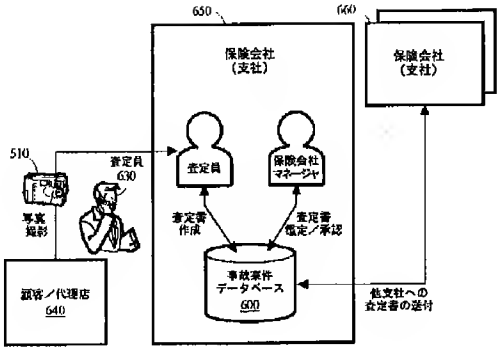
【図４０】



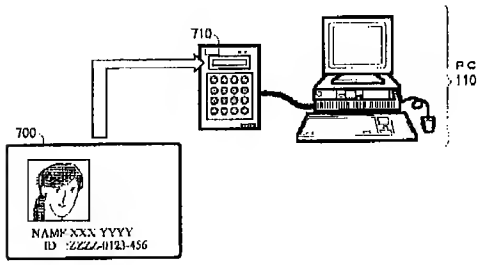
【図４３】



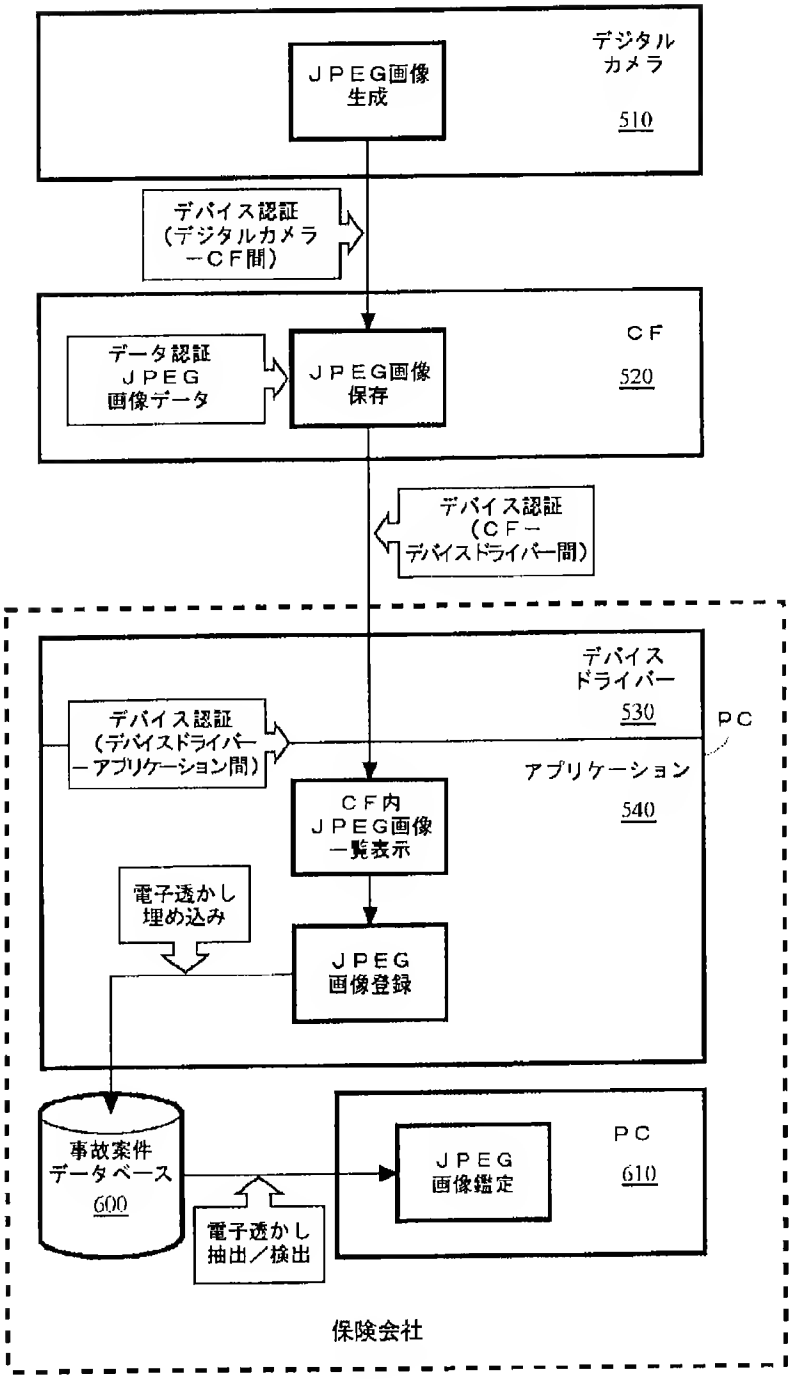
【図４４】



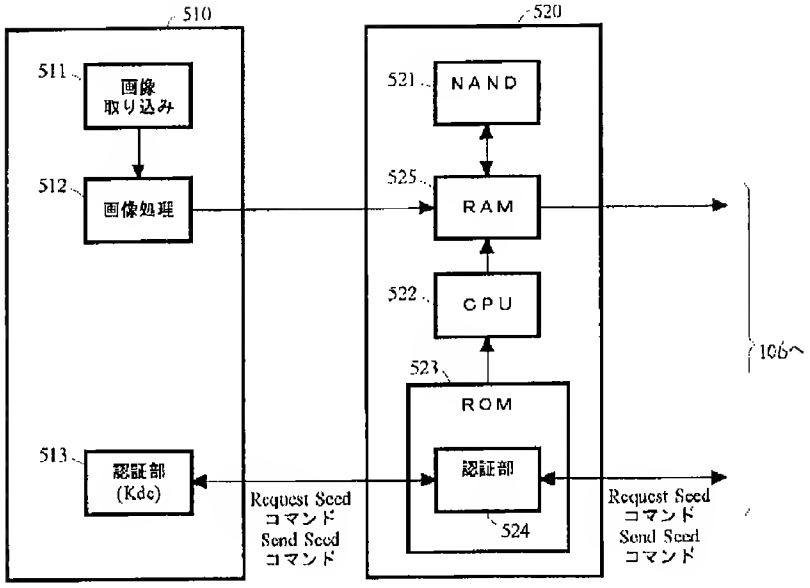
【図４７】



【図45】


デジタル
カメラ
510
JPEG画像
生成
デバイス認証
(デジタルカメラ
ーCF間)
CF
520
データ認証
JPEG
画像データ
JPEG画像
保存
デバイス認証
(CF-
デバイスドライバー間)
デバイス
ドライバー
530
PC
デバイス認証
(デバイスドライバー
ーアプリケーション間)
アプリケーション
540
CF内
JPEG画像
一覧表示
電子透かし
埋め込み
JPEG
画像登録
事故案件
データベース
600
PC
610
JPEG
画像鑑定
電子透かし
抽出/検出
保険会社

【図46】



フロントページの続き

(72)発明者　豊川　和治
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　東京基礎研究所内
(72)発明者　森本　典繁
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　東京基礎研究所内
(72)発明者　利根川　聡子
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　東京基礎研究所内

Fターム(参考)　5C053 FA13 FA27 GB06 GB07 GB22
GB36 JA21 JA22 JA30 KA24
LA06 LA14
5C076 AA02 AA14 BA03 BA06